Privacy Notice for Member Onboarding

This Data Privacy notice is effective as and from July 2021

This privacy notice explains how East Coast Credit Union, (the "Credit Union", "we", "us" and "our") use your personal information when you initiate the process of opening an account with us through our Mobile banking app.

Introduction

It is important that you are informed before you proceed with this Member Onboarding application. The app provides our members with access to online banking functionality via a mobile app interface. The online member onboarding introduces a functionality that will be openly accessible to anyone who downloads the app and will not require login.

In this Privacy Statement we explain how East Coast Credit Union deals with information which we collect about you or you provide to us while using our Mobile Banking app or when communicating with us through other interactive channels. We are committed to protecting your privacy and to ensuring that your personal information is treated in a fair, secure and lawful manner in any dealings with us.

Data protection has always been a priority for us and a core part of our business is keeping the data you entrust to us secure. We will always comply with the General Data Protection Regulation ("GDPR") when dealing with your personal data.

Credit Union Contact Details

Address	East Coast Credit Union Limited, Main Street Bray, Co Wicklow
Phone	Bray Branch - 01 2862624 Wicklow Branch - 0404 69 380
Email	info@eastcoastcu.ie
Website	www.eastcoastcu.ie

Data Protection Officer Contact Details

Phone	Phone 01 2862624
Email	Email DPO@eastcoastcu.ie

Downloading and using the East Coast Credit Union Mobile Banking App

To download and use our Mobile Banking app, you are required to register and activate the service. We will process your Personal Information during this registration and activation stage and we will transmit an activation code to the mobile number provided by you for this purpose.

East Coast Credit Union will require access to the camera on your digital device for specific purposes, for example, to allow you to photograph and upload your proof of ID and proof of address documentation and to verify these documents. Members scan their ID documents to the app; data is extracted from the identity documents to assess their authenticity.

The app will also require you to take a selfie, in the process of taking the selfie, the app, captures a short video containing hundreds of still shots. Informed AI automatically selects the best image to perform advanced facial scanning. It compares the user's facial biometrics to the photo on the ID document and generate two scores: one for validity and one for facial similarity.

The validity score tells whether the selfie is a valid, live selfie — not a pre-recorded video, bot or deep fake. The similarity score, which is also powered by informed AI, indicates the confidence level that the image in the selfie matches the photo in the identity document. If the similarity score is too low, we alert you to the possibility of impersonation fraud. We will not access your camera without your knowledge or permission and will only access it for the purposes notified to you.

Can anyone use the APP?

The app is not designed to consider applications for Under 16s. The app will not process membership applications from someone other than you, so it cannot process third-party membership applications on your behalf. Therefore, you are the sole source of the data provided during the onboarding process.

Progress Banking Systems

Progress Banking is installed in many credit unions in Ireland. They provide all the functionality and services required to process your onboarding membership application with East Coast Credit Union. Their data protection role is the processor of the data they provide the app functionality through the banking software system.

Jumio

Progress has a contract with Jumio their data protection role is a sub-processor of the data, they process identity documentation, (name, address, DOB, age) and biometric measurements to verify identity documents. A risk assessment was carried out and closely examined their use of Jumio which is a Californian based company having its operations in the US. You can learn more about Jumio by going to their website at https://www.jumio.com/compliance-regulations/.

They process the Biometric data necessary to establish your identity. Some web and mobile data will also be shared but this is limited to data about the download and usage of the app and does not include any of your data collected for the purposes of the membership application.

Collection of data

The collection of data is triggered when a user downloads the mobile app and initiates a membership application. The same information is collected as would be currently collected when someone applies in branch or in head office to join us. However, app related data is collected when someone downloads and uses the onboarding app. This data may include unique identifiers. Another difference is that documents can be provided electronically through the app.

You still, however, have the option to join in person at head office or in branch. The lawful bases for processing your data through the Onboarding app are the same as the lawful bases for processing in-branch membership applications (with the exception that in-branch applications do not include special category biometric information).

Source of the data

The data is either collected from the app user directly or generated because of their actions (date and timestamps / application status information)

Is providing your personal information obligatory?

We are unable to enter or administer the relationship with you without some personal information about you. In cases where providing your personal information is optional, we will make this clear. It is not mandatory that our members sign up to receive marketing communications.

The use of biometric information is optional and will require your explicit consent, alternatively you can complete the application by verifying your ID documentation using the normal paper process in our branch.

Types of personal data we process

The collection of the data is triggered when you download the mobile app. The data is either collected from the you directly or generated because of your actions (date and timestamps / application status information).
As mentioned above, you have an option to partially complete your membership application via the app, and to provide proof of ID, proof of address and proof of PPSN documentation in person in our branch. The information to be collected via the app is as follows:

- Personal details like your name, date and place of birth.
- Contact details like your home address (and previous addresses), email and phone number.
- Information about your right to live in the Republic of Ireland and your tax residency.
- Financial details, such as your employment status and the industry you work in, source of funds and source of wealth.
- Membership Application Status: Status of the membership application in Progress Banking.
- Mobile Number: User's mobile number.
- Mobile Number Validation Date: Date Time the user has successfully verified the mobile number via the verification code sent by SMS.
- Information about your identity, such as a copy of your ID document.
- Biometric data, which is used to verify your ID documents.

Processing of special category data – Biometric data

For the purposes of this Privacy Statement, 'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images. Biometric technology enables us to verify that the ID document truly belongs to the person making the application. Biometrics adds a critical layer of protection against stolen IDs and impersonation attacks. Your explicit consent will be required for the processing of special category of data.

The use of biometric information is optional and you can alternatively complete the application by verifying your ID documentation using the normal paper process in our branch.

Why do we collect personal data?

So that we can provide a more enhanced service. The service will also offer several efficient online services including an online banking service. You can use the app at your own convenience from home and you won't need to call into branch. The service will facilitate East Coast Credit Unions membership growth and facilitates our strategic objectives to benefit all our members.

We also gather and process your personal information for a variety of other reasons. For example, we use your personal information to process your membership application and (if your application for membership is successful) to: open an account, to maintain an account for you, to help administer your accounts and services, and to ensure we provide you with the best service possible, to prevent unauthorised access to your account and to meet our legal and regulatory obligations.

Some of these grounds for processing will overlap and there may be several grounds which justify our use of your personal data during the member onboarding process and for your relationship with us thereafter. Please do read our other privacy notices on our website which are all designed to inform you. We will also require information to comply with our obligations under Credit Union Standard Rules.

So, what are the legal bases for processing your data?

1. To comply with a legal obligation

Some of the processing of your data is required to comply with a regulatory requirement such as Anti-Money Laundering (AML) or tax regulations. When we process a membership application, we must comply with the Credit Union Act and with Anti-money laundering laws. Our legal obligations therefore apply to the Member onboarding process and indeed for your relationship with us afterwards.

The following are some of the legal obligations we have:

a) **Regulatory authorities:** to report and respond to queries raised by regulatory authorities, law enforcement and other government agencies such as the Central Bank of Ireland.

b) **Credit Union rules:** To meet our obligations under Credit Union Standard Rules.

c) **Tax Regulation compliance:** to comply with tax regulations that require us to report the tax status of our members. We may share information and documentation with domestic and foreign tax authorities to establish your liability to tax in any jurisdiction. Where a member is tax resident in another jurisdiction East Coast Credit Union has certain reporting obligations to Revenue under the Common Reporting Standard. Revenue will then exchange this information with the jurisdiction of tax residence of the member. We shall not be responsible to you or any third party for any loss incurred because of us taking such actions. Under the "Return of Payments (Banks, Building Societies, Credit Unions and Savings Banks) Regulations 2008", credit unions are obliged to report details to the Revenue in respect of dividend or interest payments to members, which include PPSN where held.

d) **Legal and Compliance:** to verify the personal information provided to us at member onboarding (and later at account opening stage) to meet our legal and compliance obligations, including to prevent money laundering, tax evasion, financing of terrorism and fraud. The information provided by you through the Member Onboarding app will be used for compliance with our customer due diligence and screening obligations under anti-money laundering and combating terrorist financing obligations under The Money Laundering provisions of the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010, as amended by Part 2 of the Criminal Justice Act 2013 ("the Act") (and any subsequent AML legislation)

e) **Duties to our Regulator:** To meet our duties to the Regulator (the Central Bank of Ireland), we may allow authorised people to see our records (which may include information about you) for reporting, and compliance purposes. For the same reason, we will also hold the information about you when you are no longer a member. We may also share personal data with certain statutory bodies such as the Department of Finance, the Department of Social Protection and the Financial Services and Pensions Ombudsman Bureau of Ireland and the appropriate Supervisory Authority, if required under law.

f) **Audit:** To meet our legislative and regulatory duties to maintain audited financial accounts, we appoint an external and internal auditor. We will allow the internal and external auditor to see our account opening and membership records (which may include information about you) for these purposes.

g) **Investigation or legal proceedings:** to co-operate with and provide information requested to legal and/or regulatory authorities in the context of investigations or proceedings.
h) **Record retention:** to keep records of communications, account opening forms and member account activities.
i) **Registration:** to maintain a register of members of East Coast Credit Union.
j) **Operations:** to administer our internal operational requirements (including membership, credit, compliance and risk management, system development, staff training, accounting and for audit purposes).
k) **Member communications:** to communicate certain information to you such as providing notice of the AGM or sending you an annual account statement.
l) **Security:** to undertake systems testing, maintenance and development to ensure network and information security.
m) **Nominations:** The Credit Union Act 1997 (as amended) allows members to nominate a person(s) to receive a certain amount from their account on their death, subject to a statutory maximum. Where a member wishes to make a nomination, East Coast Credit Union must record personal data of nominees in this event.
n) **Incapacity to Act on your account following a successful onboarding membership application:** The Credit Union Act 1997 (as amended) provides, in the circumstances where you become unable to transact on your account, due to a mental incapability and no person has been legally appointed to administer your account, that the Board may allow payment to another who it deems proper to receive it, where it is just and expedient to do so, in order that the money be applied in your best interests. To facilitate this, medical evidence of your incapacity will be required which will include data about your mental health. This information will be treated in the strictest confidentiality.

2. To enter and perform a contract with you for the services which you require

Processing through the app is also carried out for the purpose of entering a contract with East Coast Credit Union and you will need to adhere to East Coast Credit Unions rules (which are the same rules used for in-branch applications). As we operate in a regulated sector, there are many contractual considerations. This basis is appropriate where the processing is necessary for us to manage your membership and accounts and credit union services.

To consider your application for membership of East Coast Credit Union (and your relationship with us thereafter) and to process any product/service applications you may make; we must gather and process some personal information during the onboarding process and some data is processed after the process and for the purpose of maintaining an account.
The following are some examples:

a) **Administrative Purposes:** We will use the information provided by you through the app, for the purpose of assessing your Onboarding application.
b) **Third parties:** An external third party (Progress Banking Systems) is required to undertake Member Onboarding operational functions on our behalf (for example our banking system). We will ensure that any information passed to such third parties will be done for the security of your data and will be protected in line with data protection law.
c) **Electronic Payments:** If you use our electronic payment services to transfer money into or out of your credit union account which you open during your membership process (such as a 'share account'} or make payments though your debit card into your, we are required to share your data with our electronic payment service provider.
d) **Member Service:** We may use information that you provide to help us improve our services to you

3. Legitimate interests, to enable East Coast Credit Union to function as a business

A legitimate interest is when we have a business or commercial reason to use your information. Specifically for the purposes of the Membership onboarding application however, the processing of your data is not carried out based on any 'legitimate Interests'. For other data processing situations based on legitimate interests (such as Telephone recordings, services Information, CCTV and Voice Recording for example) please see our long Privacy Notice on our website.

4. Consent

The processing of additional information via the app, especially the biometric information, is optional and you can alternatively complete the application by verifying your ID documentation using the normal paper process in our branch. Explicit consent is a valid lawful basis for processing your data under Art 9 of the GDPR. Through the app we therefore seek your consent for the use of the Biometric data.

We also seek your consent for electronic AGM notifications, annual account statements, and online access. We will only carry out processing when we have obtained your express consent and will cease processing once you withdraw such consent. You can at any time withdraw consent by contacting us. Full contact details are provided at the start of this notice. For other data processing contexts that reply on your express consent, see our General Data Protection Privacy Notice on our website. Other consent options arising for you through the onboarding app also includes text marketing consent, mail marketing consent, Phone marketing consent, Post marketing consent, Members monthly Draw.

How does the Credit Union make use of Automated Decision Making?

We sometimes use automated decision making to enable us to deliver decisions within a shorter time frame and to improve the efficiency of our processes. we can give you a East Coast Credit Union account based on your age, residency, and other circumstances, like the results of anti-money laundering and sanctions checks.

AI and verification experts are used together to verify IDs in real time. If authentic, members are cleared to proceed. This is a hybrid approach to online identity verification, combining machine learning, AI, computer vision and biometrics, coupled with human review, it can provide much greater transparency about the rationale for acceptance or rejection for any given identity verification transaction.

Who do we share your data with?

We sometimes share your personal information with trusted third parties who perform important functions for us based on our instructions and applying appropriate confidentiality and security measures. For example, we may share your personal information with the following third parties:

- Any sub-contractors, agents or service providers engaged by the Credit Union (including their employees, directors and officers), such as back up and server hosting providers, IT software and maintenance providers, document storage providers and suppliers of other back office functions.
- Know Your Customer (KYC) service providers that help us with identity verification or fraud checks for example Jumio.

Who else do we share your data with?

We limit the disclosure of your information to regulatory disclosures e.g., Central Bank, CCR, MLRO Reporting and Revenue. For details of other processors who we may share your data with (following a successful Member Onboarding application), see our Data Privacy Notice on our website www.eastcoastcu.ie.

Where we store or send your data

We may transfer and store the data we collect from you to organisations outside the European Economic Area ('EEA'). When we do this, we make sure that your data is protected and that:

- the European Commission says the country or organisation has adequate data protection, or
- we've agreed to standard data protection clauses approved by the European Commission with the organisation processing the data.

Through this app, Data is transferred across borders outside the European Union. The sub-processor (Jumio) is US based, so there is potential for your data being transferred to the US and India. Transfer mechanisms as well as information about the processing locations were therefore examined as part of the risk assessment conducted and no high residual risks were found.

Security

We use internal technical and organisational measures to protect your information from unauthorised access, to maintain data accuracy and to help ensure the appropriate use of your Personal Information by East Coast Credit Union.
Our providers are also bound by confidentiality obligations. Identity verification is very important in the new member onboarding process, and this app provides two mechanisms to ensure that this verification can be achieved through the online process (a) validation of your mobile phone associated with the account and (b) verification of your identity document through Jumio. This is done via a one- time-password generated and sent to you via SMS. You must type this password and send it back to the server for validation. The password has an expiry period. A desk-based assessment was carried out on Jumio

Progress Systems have been assessed and certified as meeting the requirements of ISO27001 for the provision of computer software, hardware and support to East Coast Credit Unions and they are subject to satisfactory surveillance audits. Vulnerability and a Penetration Tests of their Internet Banking Service is regularly conducted to ensure there is no risk to data. Progress' Information Security Management System (ISMS) was certified to ISO/IEC 27001:2005 in 2012. In 2015 they upgraded their ISMS to the ISO/IEC 27001:2013 standard. Each year their ISMS has been subject to a surveillance audit to ensure adherence to the ISO 27001 standard ensuring the highest awareness of data protection for East Coast Credit Union Ltd.

There is also an existing Data Processing agreement between East Coast Credit Union and Progress Software which incorporates the member onboarding processing activity. Access controls are enforced by our banking software and the data collected is processed within our banking software. We do not allow our third-party service providers to use your personal data for their own purposes, unless they are deemed to be controllers. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

Data is shared between the app, Progress Banking system and the sub-processor (Jumio) using encrypted links. Jumio and Progress (our banking software providers) encrypt all your data in transit and Jumio encrypts all your data 'at rest'. All our third-party service providers are required to take these appropriate security measures to protect your personal data in line with our policies.

The ID verification software is PCI-DSS Level 1 compliant, it regularly subjects its security practices to stringent regulatory security audits, vulnerability scans, and penetration tests to ensure compliance of the product. All personal data, including ID documents and selfies is encrypted twice: all data is encrypted in transit via TLS encryption using strong cipher suites and at rest with military-grade 256-bit AES encryption.

App penetration tests have been carried out and will be ongoing to ensure the integrity of your data. Only Irish Mobile numbers are used which restricts opportunities for fraudulent use of your data. All data is always encrypted in transit and on the banking system.

How long do we hold your data?

Our ID verification software is PCI DSS compliant; it is already mandated to adhere to strict data retention procedures ensuring that personal data that is no longer needed is discarded appropriately and in a timely fashion, within 5 days.
We keep most of your data as long as you're a member of East Coast Credit Union, and for 6 years after that to comply with the law and if we face a legal challenge. In some circumstances, like cases of anti-money laundering or fraud, we may keep data longer if we need to (that's in our legitimate interest) and/or the law says we must. To work out how long we keep different categories of data, we consider why we hold it, how sensitive it is, how long the law says we need to keep it for, and what the risks are.

Your rights under Data Protection law

Providing and holding personal information comes with significant rights on your part and significant obligations on ours. You have several rights in relation to how we use your information. If you make your request electronically, we will, where possible, provide the relevant information electronically unless you ask us otherwise:

1. The right to be informed

To know how your data is processed, stored, deleted and transferred

2. The right to access information

To access your information and to receive copies of the information we have about you. Under the new data protection regulations, we are obliged to respond to your access request without undue delay. In most instances, we will respond within 30 Days. If we are unable to deal with your request fully within 30 Days (due to the complexity or number of requests), we may extend this period by a further two calendar months. Should this be necessary, we will explain the reasons why. If you make your request electronically, we will, where possible, provide the relevant information electronically unless you ask us otherwise.

3. The right to rectification

Request that inaccurate information is corrected and incomplete information updated.

4. The right to be forgotten

Request that your data is erased if one of the following grounds applies: it's no longer necessary in relation to the purpose for which it was collected, your consent was withdrawn, you object to processing or the processing is unlawful.

5. Right to data portability

Obtain a transferable copy of certain data to which can be transferred to another provider, known as "the right to data portability".
This right applies where personal information is being processed based on consent or for performance of a contract and the processing is carried out by automated means. You are not able to obtain through the data portability right all the personal information that you can obtain through the right of access.

The right also permits the transfer of data directly to another provider where technically feasible. Therefore, depending on the technology involved, we may not be able to receive personal data transferred to us and we will not be responsible for the accuracy of same.

6. The right to object to the processing of personal data

Object to use of your personal data for direct marketing purposes. If you object to this use, we will stop using your data for direct marketing purposes.
Withdraw consent at any time, where any processing is based on consent. If you withdraw your consent, it will not affect the lawfulness of processing based on your consent before its withdrawal.

7. The right of restriction

Have your data deleted or its use restricted - you have a right to this under certain circumstances. For example, where you withdraw consent, you gave us previously and there is no other legal basis for us to retain it, or where you object to our use of your personal information for legitimate business interests.

8. The right not to be subject to automated decision making, including profiling

Object to uses of your personal data where the legal basis for our use of your data is our legitimate business interests (for example, profiling we carry out for our legitimate business interests) or the performance of a task in the public interest. However, doing so may have an impact on the services and products we can / are willing to provide.
Please note that the above rights are not always absolute, and there may be some limitations
If you want access and/ or copies of any of your personal data or 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 send you or a third party a copy your relevant personal data in a reusable format, if you have any questions about how your personal data is gathered, stored, shared or used, or if you wish to exercise any of your data rights, please contact our Data Protection Officer at:

Data Protection Officer Contact Details

Phone	Bray Branch - 01 2862624 Wicklow Branch - 0404 69 380
Email	DPO@eastcoastcu.ie

Under Article 77 of the GDPR, you have the right to lodge a complaint with the Data Protection Commission or another supervisory authority if you consider that processing of your personal data is contrary to the GDPR.

Data Protection Commission Contact Details

Postal Address	Data Protection Commission, 21 Fitzwilliam Square South, Dublin 2, D02 RD28
Website	www.dataprotection.ie
Phone	(01) 765 0100 or 1800 437 737
Email	info@dataprotection.ie

Where do I get more information?

If you have any questions about GDPR or your personal information, please contact DPO@eastcoastcu.ie
Further details on the GDPR can be found at Office of the Data Protection Commissioner's website (www.dataprotection.ie)
We reserve the right to amend this Privacy Notice from time to time without prior notice. You are advised to check our website www.eastcoastcu.ie or our branch regularly for any amendments.