Detailed Privacy Notice

Introduction

This Privacy Notice provides information about the ways in which Carrick-on-Suir Credit Union collect, use, secure, retain, share and update the personal data provided by our members and any other individuals.

We are a data controller for the purposes of the Data Protection Acts 1988 to 2018 ("the Acts") and the General Data Protection Regulation ("the GDPR"). As a data controller, we respect and protect the privacy of all individuals whose data we process. We ensure that all processing of personal data is carried out in line with the principle of data processing and our obligations as a data controller.

Should you require further details about how we process your personal data please contact us using the details at the end of this notice.

Principles of Data Processing

We are responsible for and must be able to demonstrate compliance with the data protection principles listed below (Accountability).

We adheres to the principles relating to Processing of Personal Data set out in the GDPR which require Personal Data to be:

Lawful, Fair and Transparent.	Processed lawfully, fairly and in a transparent manner
Purpose Limitation.	Collected only for specified, explicit and legitimate purposes
Data Minimisation.	Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed
Data Accuracy	Accurate and where necessary kept up to date
Storage Limitation	Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed
Security, Integrity and Confidentiality.	Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage
Accountability	We are responsible for and must be able to demonstrate compliance with the data protection principles listed above

Lawfulness of Processing Personal Data

The GDPR allows processing where you have a legal basis for doing so. We will identify and document the legal ground being relied on for each processing activity. This information is held in our Personal Data Register and is displayed on our Privacy Notices.

Examples of how we use the lawful bases outlined above when processing personal data are:

Article 6.1(b) GDPR "*processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract*"

Examples of where this lawful basis is applicable include the following:

- the processing is necessary for us to manage accounts and services provided to our members;
- for the purpose of assessing any loan application, processing applications individuals make and to maintain and administer any accounts held with us;
- to take steps to secure repayment of a loan where a loan goes into arrears;
- to apply for Loan Protection;
- to process a credit assessment when a member applies for a loan;
- to perform any part of a contract as per the Terms and Conditions outlined to our members in any such process.

Article 6.1(c) GDPR "*processing is necessary for compliance with a legal obligation to which the controller is subject"*

Examples of where this lawful basis is applicable include the following:

- to comply with the all regulations as outlined in the Credit Union Act 1997 (as amended);
- to meet our duties to the Regulator, the Central Bank of Ireland;
- to fulfil reporting obligations to Revenue related to a member's tax liability under Common Reporting Standard;
- to comply with 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;
- to meet our legislative and regulatory duties to maintain audited financial accounts;
- to comply with credit reporting obligations;
- to comply with Connected/Related Party Borrowers obligations;
- to appoint a person to administer an account where a member becomes mentally incapacitated;

Article 6.1(f) GDPR "*processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party"*

Examples of where this lawful basis is applicable include the following:

- assessing a loan application, as well as fulfilling a contract mentioned above, we also utilise credit data from credit referencing agencies. Our legitimate interest: We must, for own benefit and therefore the benefit of our members, must lend responsibly and will use credit scoring information in order to determine suitability for a loan;
- where there is a breach of a loan agreement we may use the service of a debt collection agency, solicitors or other third parties to recover the debt. Our legitimate interest: We will, where appropriate, take necessary steps to recover a debt to protect the assets and equity of the credit union;
- when carrying out searches relating to credit worthiness. Our legitimate interest: We must, for our own benefit and therefore the benefit of our members, must lend responsibly and will use credit scoring information in order to determine loan suitability;
- CCTV recording on our premises. Our legitimate interest: it is necessary to secure the premises, property herein and any staff /volunteers/members or visitors to our premises and to prevent and detect fraud;
- voice recording through phone conversation both incoming and outgoing. Our Legitimate interest: To ensure a good quality of service, to assist in training, to ensure that correct instructions were given or taken due to the nature of our business and to quickly and accurately resolves any disputes;
- during a recruitment process when we need to communicate with candidates. Our Legitimate interest: to update candidates on the recruitment process for the purposes of considering them for employment or for future positions;
- when we use data analytics. Our legitimate interest: to ensure we are offering relevant services , to assess demand for certain services and to ensure we are acting in the best interests of the credit union. We utilise data analytics to analyse our common bond performance. This analysis, conducted by a trusted

third-party provider under contract, ensures that we act in the legitimate interests of our members, who are the ultimate owners of the credit union, and safeguards the financial stability of the credit union into the future. It is important to note that we do not use data in its original state where individuals can be identified, and no analytics are carried out prior to anonymisation of the data. If you are not happy with your data being processed in this manner, you have the right to object by contacting us using the details provided below.

Article 6.1(e) GDPR "*processing is necessary for the performance of a task carried out in the public interest*"

Examples of where this lawful basis is applicable include the following:

- processing of data relating to compliance with guidance from Public Health Authorities during the Covid-19 pandemic

Article 6.1(a) GDPR "*the data subject has given consent to the processing of his or her personal data for one or more specific purposes*"

Examples of where this lawful basis is applicable include the following:

- **Marketing:** to provide our members with details on our products and services provided they have not opted out of receiving such communications. Individuals can opt-out of receiving marketing communications at any time;
- **Competitions and Draws:** when members participate in competitions or draws they will be asked for their consent prior to their personal information or image being displayed on our website, social media platforms or other publications;
- **Cookies on our website:** we may obtain information about general Internet usage by using a cookie file which is stored on an individual's browser or the hard drive of their computer. Visitors to our website can choose not to consent to cookies, or they can manage their cookie preferences, or they can select to opt-in to some or all types of cookies. We use a cookie management platform for this purpose.
- **AIS Process:** if a member avails of the AIS (Account Information Service) process as part of a loan application, the AISP (Account Information Service Provider) Truelayer Ireland Limited, will look for consent to consent to retrieve your bank account information and to share this with us. For the purposes of this process, Truelayer are an independent data controller.

Purposes for Processing Personal Data

Types of Personal Data

We hold personal data about our members, our staff, service providers, suppliers and other individuals for a variety of purposes. The personal data held by us includes the following:

Credit union account number, details of the products you hold, Address data, bank data, contract data, signatures, identification documents, date of birth, email, telephone, salary, occupation, financial information, accommodation status, mortgage details, previous addresses, spouses, partners, nominations, PPSN/National Insurance numbers individuals' contact and address details, passport details, date of birth, beneficial owners, connected party details, credit history, interactions with our staff on the premises, CCTV footage, by phone or email, current or past complaints, educational background, financial and pay details, details of certificates and diplomas, education and skills, nationality, job title, and CVs.

Account Opening:

We will use personal data in order to carry out the following functions related to opening an account:

- To open and maintain an account;
- To give consideration to an application prior to approval;
- Verifying the information provided in the application;

- To comply with our legal obligations, for example anti-money laundering, to identify connected borrower, to identify a politically exposed person, to submit information account information to the Central Bank;
- To confirm tax residency for the purposes of the Common Reporting Standard;
- To meet our obligations under the Credit Union's Standard Rules;
- To provide members with details of the Deposit Guarantee Scheme;
- To contact members in respect of their accounts;
- To contact members in relation to any operational matters within the credit union;
- To record details of nominations and to process the nomination (subject to a valid nomination) and transfer any nominated property to the nominee(s);
- To issue members with information on our products or services or to provide details of other services, products, offers or competitions that may be of interest to our members.

Loans: Applications, Administration and Arrears:

We will use personal data in order to carry out the following functions:

- Assessing a loan application and determining creditworthiness for a loan;
- Verifying the information provided in the application;
- Conducting credit searches and making submissions to Irish Credit Bureau, the Central Credit Register;
- To purchase loan protection from ECCU;
- To determine whether an applicant is a connected borrower or related party borrower in order to comply with Central Bank Regulations;
- Administering the loan, including where necessary, to take steps to recover the loan or enforce any security taken as part of the loan;
- To take steps to secure repayment of a loan such as processing a charge on a property;
- Providing updates on loan products and services by way of directly marketing to members;
- To contact members regarding a loan enquiry submitted through our website or online advertising;
- To contact members in relation to any transactions or missed payments on their account;
- Meeting legal and compliance obligations and requirements under the Rules of the Credit Union;
- To submit data to the Central Credit Register where a loan falls into arrears;
- To thank members for completing their loan payments in full;
- Where there is a breach of the loan agreement, we may use the service of a solicitor to recover the debt. We will pass them details of the loan application in order that they make contact and details of the indebtedness in order that they recover the outstanding sum;
- To enable members to avail of AIS (Account Information Service) process to share their bank account transactions with us as part of a loan application. This process is carried out by an Independent Data Controller (Truelayer) and consent will be obtained by Truelayer;
- In order to locate members whose loans fall into arrears and who will not engage with us, we may use information from public sources to make contact with them to pursue monies owing.

Guarantors: As part of the conditions of a loan, the appointment of a guarantor may be a requirement in order to ensure the repayment of a loan. In such instances, we have a legal and regulatory requirement to collect, process and store certain personal data of the guarantor. This will include data such as:

- name, address, contact details, occupation, salary and other relevant financial data.

The purposes for which we may process the data of the guarantor include:

- ensure the terms of the loan agreement are met
- to contact the guarantor if the loan falls into arrears or there is a change in the payments by the member that indicate a change in circumstances
- to collect the debt
- to carry our required credit searches

The loan balance may be communicated to the guarantor at any time for the duration of the loan. The details of the guarantor will be retained in line with the loan which is 7 years from the date the loan is paid in full.

General Administration and Operation

We will use personal data to assist it in carrying out the following:

- To resolve complaints and improve service standards;
- To contact members to thank them for their custom, particularly in relation to the completion of a loan;
- To contact members, using any contact method supplied, about reactivating dormant accounts;
- To record CCTV footage to ensure the safety and security of our staff, members, volunteers and any other third parties visiting our premises, to resolve complaints and improve service standards;
- To collect certain personal data if members attend the AGM such as name, account number and signature;
- To issue obligatory information to members (eg. AGM notifications, annual accounts and certain reports);
- To collect member preferences regarding marketing materials;
- Providing updates on our products and services by way of directly marketing to members;
- From time to time we may collect a small amount of personal data for entry into competitions and prize draws e.g. Car Draw. We will only use this data for the purpose of determining entry and selecting a winner for the competition/draw. Any photographic images or videos processed during participation in competitions or draws will only be done so with specific consent;

We may process data for purposes that are not specifically outlined above. If we do, we will clearly outline the purposes at the time of collecting data. We will endeavor to explain these purposes when we collect this data. We use personal information for the purpose it was collected. We do not use personal information for any different purpose other than for what it was obtained for without notification and seeking permission first.

Online Operations

We offer a number of online services to our members and prospective members. In order to avail of our online services, members or prospective members must provide certain personal information.

This information is required to:

- Login to the online platform;
- Use our Mobile App;
- Transfer funds;
- Manage payments and payees;
- Apply for a loan;
- Upload loan supporting documentation;
- Upload updated ID and POA documents;

Specific Terms and Conditions apply to the usage of our online platforms and we would advise users to read these and contact us with any queries.

"Special Categories" of Data

In order to provide certain services, it may be necessary for us to process some "special categories" (see definition above) of personal data. "Special categories" of particularly sensitive personal data require higher levels of protection.

We need to have further justification for collecting, storing and using this type of personal data. We may process special categories of personal data in the following circumstances:

- In limited circumstances, with explicit written consent;
- Where we need to carry out our legal obligations and in line with our data protection policy;
- Where it is needed in the public interest, and in line with our data protection policy;
- We may process this type of information where it is needed in relation to legal claims or where it is needed to protect a member's interests (or someone else's interests) and a member is not capable of giving their consent, or where this information has already been made public;
- In certain circumstances, where a member becomes unable to transact on their account due to a mental incapability and no person has been legally appointed to administer the account, the Board may allow

payment to another person who it deems proper to receive it, where it is just and expedient to do so, in order that the money be applied in the member's best interests. In order to facilitate this, medical evidence of the member's incapacity will be required which will include data about their mental health. This information will be treated as strictly confidential.

Data Subject's Rights and Requests

Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

a	**withdraw** Processing based on Consent at any time;
b	**receive** certain information about the Data Controller's Processing activities;
c	**request** access to their Personal Data that we hold;
d	o**bject** to our use of their Personal Data for direct marketing purposes;
e	**ask us to erase** Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;
f	**restrict** Processing in specific circumstances;
g	**object to** Processing which has been justified on the basis of our legitimate interests or in the public interest;
i	**object** to decisions based solely on Automated Processing, including profiling (ADM)[1];
k	be **notified** of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;
l	**make a complaint** to the supervisory authority; and
m	**in limited circumstances, receive or ask** for their Personal Data to be transferred to a third party in a structured, commonly used and machine readable format[2].

Data Access Requests

An individual has the right to be informed whether we hold data/information about them and to be given a description of the data together with details of the purposes for which their data is being kept. The individual should make this request to us in writing, and we will accede to the request within one month having first verified the identity of the requester to ensure the request is legitimate.

Where a subsequent or similar request is made soon after a request has just been dealt with, it is at the discretion of the controller whether or not it needs to comply with the second request. This will be determined on a case-by-case basis. In cases where we process a large quantity of information concerning the data subject, we may request that, before the information is delivered, the data subject specify the information or processing activities to which the request relates.

No personal data can be supplied relating to another individual unless that third party has consented to the disclosure of their data to the applicant. Data will be carefully redacted to omit references to any other individual and only where it has not been possible to redact the data to ensure that the third party is not identifiable, we must refuse to furnish the data to the applicant.

Individuals are asked to complete our Data Access Request form when making a request, though it is not mandatory. Once we have verified the identity of the requester and the request is not deemed to be manifestly unfounded or excessive, we will comply with the request at no charge to the data subject and within one month.

We have an internal procedure in place to handle all Data Access Requests.

[1] This right does not apply when the automated decision is: Necessary for entering into or performing a contract with the data subject; authorised by EU or member state law applicable to the data controller if the law requires suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or based on explicit data subject consent.

[2] The right only applies to: Personal Data provided by the data subject or generated by their activity where the legal basis of processing is consent/contract and where the data is processed electronically.

Data Sharing and Transfers

Sharing of Personal Data

Generally, we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

Our staff may only share the Personal Data we hold with another employee, officer agent or representative of the credit union (if the recipient has a job/position-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.)

We will ensure that any information passed to third parties conducting operational functions on our behalf will be done with respect for the security of personal data and will be protected in line with data protection law.

Ways in which we may share personal information include:

- With official bodies including, but limited to:
  - the Irish League of Credit Unions (ILCU) under the ILCU Standard Rules and the League Rules which govern the operation of Credit Unions;
  - ECCU Assurance DAC who provide Loan Protection and personal data must be shared in order to administer claims or deal with insurance underwriting;
  - The Central Credit Register who provide financial institutions with credit details relating to a member's eligibility for a loan;
  - The Central Bank of Ireland (CBI) enforce certain reporting, compliance and auditing on Credit Unions. We are obliged, further to CBI Regulations, to identify where borrowers are connected in order to establish whether borrowers pose a single risk. We are also obliged to establish whether a borrower is a related party when lending to them, i.e. whether they are on the Board/Management Team or a member of the Board/ Management teams family or a business in which a member of the Board /Management Team has a significant shareholding. Further reporting obligations include submitting the name, date of birth, address, beneficial owner and IBAN for every credit union account to the CBI;
  - Government Departments such as Department of Finance and the Department of Social Protection may require us to share certain personal information in order to meet legislative and regulatory requirements;
  - The Revenue Commissioners impose certain reporting obligations on Credit Unions under the Common Reporting Standards in relation to tax residency and the in respect of dividend or interest payments to members.
- To engage external IT providers so as to ensure the security of our IT systems in order to protect all personal data;
- If members avail of the AIS process as part of a loan application, they will be sent a link to the provider's portal (Truelayer Ireland Limited) where they will be asked to consent to retrieve their bank account information and to share this with us. For the purposes of this process, Truelayer are an independent data controller and full details about this process are on our website. They are regulated by the Central Bank of Ireland. Please refer to Truelayer's privacy policy available at this link: *https://truelayer.com/en-ie/legal/privacy/.*
- To engage debt collectors to assist us in pursuing members who are in arrears on their loan and will not engage with us directly;
- With our insurers or assessors when providing or reviewing information in the event of an incident occurring;
- To engage professional services of third parties, such as auditors, solicitors or any other such business advisers. Any such parties are bound by confidentiality;
- With any relevant, authorised third parties as part of a merger or transfer of engagment, any such parties will be bound by a duty of confidentiality;

- We reserve the right to report to law enforcement any activities that we, in good faith, believe to be illegal;
- To provide information to An Garda Síochána (eg. CCTV footage) or other Government bodies or agencies when required to do so by law; and
- To transfer data to another credit union where we have received a request, authorised by you, from another credit union to do so.

Data Transfers

There may be circumstances where we transfer your personal data outside the EEA, such as when we use the services of online platforms or where we use a cloud-based IT system to hold your data.

We safeguard your data by ensuring a minimum of one of the following safeguards is in place:

- a contract based on "model contractual clauses" (also called Standard Contractual Clauses) approved by the European Commission, obliging them to protect your personal data;
- with companies who have approved Binding Corporate Rules approved by the European Commission; or
- with companies located in a third country approved by the European Commission under an adequacy decision.

Prior to any transfer of personal data, we will ensure that the transfer is necessary for one of the other reasons set out in the GDPR including the performance of a contract between us and the Data Subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent and, in some limited cases, for our legitimate interest.

Where any of our suppliers engage the service of sub-processor to process data of which we are a Data Controller, our due diligence measures will include an assessment of this processor, in particular where the processor is located outside the EEA.

Data Retention

We will only retain personal data for as long as necessary to fulfil the purpose(s) for which it was obtained, taking into account any legal/contractual obligation to keep it. Where possible we record how long we will keep your data, where that is not possible, we will explain the criteria for the retention period. Once the retention period has expired, the respective data will be permanently deleted.

As a general rule, personal information will be retained for 7 years from the date an account is closed. Where members apply for a loan, the documentation required for this will be retained for a minimum of 5 years from the date the loan is completed. However, they may be circumstances where we must retain data for longer than these specified periods, but we will always have a defined legitimate basis for any extended retention.

We maintain a full Retention Schedule in our Records Management Policy.

Privacy by Design and Data Protection Impact Assessment (DPIA)

We are required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures (like Pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.

Our staff will assess what Privacy by Design measures can be implemented on all programs /systems/ processes that Process Personal Data by taking into account the following:

- the state of the act;
- the cost of implementation;
- the nature, scope, context and purposes of Processing; and
- the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the Processing.

We will also conduct DPIAs in respect of any processing which is considered to be high risk.

We must conduct a DPIA (and discuss any findings with the Data Protection Officer) when implementing major system or business change programs involving processing we deem to present a risk to individuals.

A DPIA will include:

- a description of the Processing, its purposes and our legitimate interests if appropriate;
- an assessment of the necessity and proportionality of the Processing in relation to its purpose;
- an assessment of the risk to individuals; and
- the risk mitigation measures in place and demonstration of compliance.

Direct Marketing

We are subject to certain rules and privacy laws when marketing to our members and non-members. We have identified consent as the legal basis upon which it will conduct direct marketing.

A Data Subject's prior consent is required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing members known as "soft opt in" allows us to send marketing texts or emails if we have already obtained contact details in the course of signing up the member or providing a loan to that person, we are marketing similar products or services, and we gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

The right to object to direct marketing is explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information.

Data Security

We are committed to protecting the personal data of our members and have implemented appropriate technical and organisational measures (TOMs) to ensure the security of this data. These measures are designed to prevent unauthorised access, disclosure, alteration, or destruction of personal information. We regularly review and update our security practices to address emerging threats and ensure compliance with applicable data protection laws. Our staff are trained in data protection principles, and we conduct regular audits and assessments to evaluate the effectiveness of our security measures, ensuring that we maintain a high standard of data security to safeguard the personal information we process and store.

Implications of not providing information

Please note that in some cases, if you do not agree to the way we process your information, it may not be possible for us to continue to operate your account and/or provide certain products and services to you.

How to contact us

If you have any questions or concerns related to our Privacy Notice, you can contact us using the below details.

- **In branch:** Greystone Street, Carrick-on-Suir, Co. Tipperary.
- **Phone:** 051 640675
- **Email:** info@carrickcu.ie / dpo@carrickcu.ie

Updates to the Notice

We may update this Privacy Notice from time to time, members are advised to always check our website for the most recent version.

This Notice was last updated in November 2024.