

## Privacy Notice of Limerick & District Credit Union Limited Credit Union Personnel

Our contact details are:

Address: Credit Union House, Redgate, Caherdavin, Limerick V94 D362

Website; [www.mylimerickcu.ie](http://www.mylimerickcu.ie)

Email: [info@lcu.ie](mailto:info@lcu.ie)

Phone: 061-455831

The Data Protection Officer for Limerick & District Credit Union Ltd can be contacted on 061-455831 or by email at [dpo@lcu.ie](mailto:dpo@lcu.ie) or at the above address.

Limerick & District Credit Union is committed to protecting the privacy and security of your personal data. This privacy notice describes how we collect and use personal data about you during and after your relationship with us ends, in accordance with the General Data Protection Regulation (GDPR).

This privacy notice is for distribution amongst all employees, workers, contractors, agency workers, consultants, directors, officer and volunteers (Credit Union Personnel) of the credit union. Please note that there may be elements of the notice that are not applicable to you according to the specific role you undertake within the credit union.

This privacy notice applies to current and former Credit Union Personnel. We may update this notice at any time.

We may collect, store, and use the following categories of personal data about you:

Personal contact details such as name, title, addresses, signatures, telephone numbers, and personal email addresses.

Date of birth.

Gender.

Your Child's Name and PPSN [*e.g. for purpose of tracking Parental Leave*]

Marital status and dependants [*for example might be required for pension purposes*]

Next of kin and emergency contact information.

PPSN/National Insurance number.

Bank account details, payroll records and tax status information.

Salary, annual leave, pension and benefits information.

Start date.

Location of employment or workplace.

Copy of driving licence.

Recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process).

Employment records (including job titles, work history, working hours, training records and professional memberships).

Compensation history.

Performance information

Disciplinary and grievance information.

CCTV footage and other information obtained through electronic means such as fob records.  
Information about your use of our information and communications systems.  
Photographs for example for use in an identification card/for identifying staff on a website etc.  
Recording of your voice  
Visa/Immigration/right to work or residential status  
Criminal offences for specific functions *\*subject to the finalisation of the national implementing legislation.*

We may also collect, store and use the following “special categories” of more sensitive personal data:  
Trade union membership.  
Information about your health, including any medical condition, health and sickness records.  
Biometric data.

### **How we collect the information**

We collect personal data about Credit Union Personnel from the following sources:

- You;
- the application and recruitment process, either directly from candidates or from third parties
- a recruitment agency, third party placement firm or job search website;
- We may sometimes collect additional information from third parties including former employers, background check provider or credit reference agencies
- References which have been provided to us

We will collect additional personal data in the course of role-related activities throughout the period of you working for us.

### **Why we collect the information and how we use it**

We will use your personal data for the following purposes:

- Where we need to perform the contract we have entered into with you;
- Where we need to comply with a legal obligation;
- Where it is necessary for our legitimate interests (or those of a third party) and your interests; and fundamental rights do not override those interests. If we rely on our legitimate interest, we will tell you what that is.

We may also use your personal data in the following situations, which are likely to be rare:

- Where we need to protect your interests (or someone else’s interests).
- Where it is needed in the public interest [or for official purposes].

### **Information provided to us by you about others or others about you**

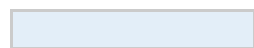
There may be instances where you provide us with someone else’s personal data or they provide us with yours. Where this occurs, it is important that you seek their approval to disclose their personal data and likewise, they seek yours. We may add it to any personal information we already hold and we will use it in the ways described in this privacy notice.

### **Situations in which we will use your personal data**

We need all the categories of information in the list above primarily to allow us to perform our contract with you and to enable us to comply with legal obligations.

In some cases we may use your personal data to pursue legitimate interests of our own provided your interests and fundamental rights do not override those interests.

The situations in which we will process your personal data are listed below.

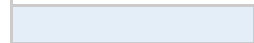


**Fulfilling contract** This basis is appropriate where the processing is necessary for us to manage our contract with you

**Recruitment:** Making a decision about your recruitment or appointment to future roles that may become available. Assessing qualifications for a particular job or task.

**Employment:** Determining the terms on which you work or volunteer for us. Conducting performance reviews, managing performance and determining performance requirements including decisions about promotions. Making decisions about salary reviews and compensation. Administering the contract we have entered into with you. Education, training and development requirements. Making decisions about your continued employment or engagement Making arrangements for the termination of our relationship. Gathering evidence for possible grievance or disciplinary hearings

**Remuneration:** Paying you and, if you are an employee, deducting tax and other legal contributions. Providing the following benefits to you where applicable: Health Insurance, Pension and Sick pay. Liaising with your pension provider, if applicable. Business management and planning, including accounting and auditing.



**Our legal duty** This basis is appropriate when we are processing personal data to comply with Irish and EU Law

**Recruitment:** Assessing your fitness to control function roles under the fitness and probity regime. Ascertaining your fitness to work and working capacity e.g. pre-employment medicals and occupational health assessments. Checking you are legally entitled to work in the Republic of Ireland

**Employment:** Complying with health and safety obligations. Dealing with legal disputes involving you, or Credit Union Personnel, including accidents at work. Gathering evidence for possible grievance or disciplinary hearings. Making arrangements for the termination of our working relationship

**Remuneration:** Compliance with social security and social protection laws e.g. processing certain data to pay sick pay, maternity benefit, paternity benefit. Recording of working hours, annual leave and public holidays.

**Tax liability:** 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 the 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 may also report member's information to comply with the Foreign Account Tax Compliance Act (FATCA). We shall not be responsible to you or any third party for any loss incurred as a result 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.

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



**Legitimate interests** A legitimate interest is when we have a business or commercial reason to use your information. But even then, it must not unfairly go against what is right and best for you. If we rely on our legitimate interest, we will tell you what that is.

To monitor your use of our **information and communication systems** to ensure compliance with our IT policies. Our **legitimate interests**. Our IT policies are in place to protect our IT infrastructure including business continuity

**CCTV:** The purpose of this is for security The purpose of this is for security, for the prevention of theft, pilferage, and for the security of the credit unions staff, officers, members, visitors, contractors and credit union property. **Our legitimate interest:** With regard to the nature of our business, it is necessary to secure the premises, property herein and any staff /volunteers/members or visitors to the credit union

To ensure **network and information security**, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution. **Our legitimate interest:** It is important to ensure continuity of service to our members and to comply with our legal and regulatory obligation that appropriate IT technical and security measures are in put in place by us.

To conduct data analytics studies to review and better understand Credit Union Personnel **retention** and attrition rates. **Our legitimate interest:** It is important that we understand our retention and attrition rates to ensure that we address any issues.

Vehicle trackers are fitted to vehicles used by some employees and the information obtained is processed by a third party provider to enable us to monitor the driver location. The third party provider retains tracking information on our behalf for 24 months to enable us to investigate any incidents.

**Vital interests:** The Processing is necessary to protect the vital interests of the data subject or another individual

Using an employee's emergency contact number. In the event of an emergency it will be necessary for us to contact your emergency contact, next of kin or other contact

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal data.

### **If you fail to provide personal data**

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our individuals undertaking a role within the credit union). If there are any changes to your personal data (e.g. a new address), you should let us know as soon as possible.

### **Change of purpose**

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

allows us to do so. This will only be done in accordance with our policies.

Please note that we may process your personal data without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

## HOW WE USE SENSITIVE 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:

1. In limited circumstances, with your explicit written consent.
2. Where we need to carry out our legal obligations and in line with our data protection policy.
3. Where it is needed in the public interest, such as relation to our occupational pension scheme, insurance or health insurance, and in line with our data protection policy.
4. Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards.

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

The Irish League of Credit Unions act as an insurance intermediary for various insurance products.

We may pass your details in the event of you having to avail of any services.

### Our obligations as an employer

We will use your sensitive personal data in the following ways:

We will use information relating to leaves of absence, which may include sickness absence or family related leaves, to comply with employment and other laws.

We will use information about your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits.

We will use trade union membership information to pay trade union premiums, register the status of a protected **employee** and to comply with employment law obligations.

We will use information about your race or national or ethnic origin to establish if we require a work permit for you to be eligible to work for us]

### Do we need your consent?

Under the General Data Protection Regulation (GDPR), the requirements for valid consent have been made much stricter. Consent must be freely-given, specific, informed and revocable. The GDPR expressly states that, where there is an imbalance of power between the party giving consent and the party receiving it, consent will not be valid. On the basis of our relationship with you, consent would not be valid. We therefore rely on other legal bases to process your personal data as set out in this privacy notice.

Where you have a genuine choice as to the processing, and in limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully

consider whether you wish to consent. You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

## **INFORMATION ABOUT CRIMINAL CONVICTIONS**

We may only use personal data relating to criminal convictions where the law allows us to do so. We will only collect personal data about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so.

We are required to carry out a criminal records check in order to satisfy ourselves that there is nothing in your criminal convictions history which makes you unsuitable for the role. In particular:

- When undertaking assessment for the Fitness and Propriety regime, you may be required to self-certify in respect of your criminal history.

Where we do process criminal data we will ensure that appropriate additional safeguards as required by the Data Protection Act 2018 are in place.

## **How we may share the information and how secure is my information?**

We may also need to share your personal data with other parties, such as HR consultants, the Irish League of Credit Unions (ILCU), insurers and professional advisers. We may also share your personal data with other third parties, for example in the context of the possible transfer, amalgamation or merger of the credit union in compliance with the applicable credit union legislation or restructuring of the credit union. All our third-party service providers are required to take appropriate security measures to protect your personal data in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes unless they are deemed to be data controllers in their own right. We only permit them to process your personal data for specified purposes and in accordance with our instructions. Usually, information will be anonymised but this may not always be possible. The recipient of the information will also be bound by confidentiality obligations. We may also need to share your personal data with a regulator, government agency or to otherwise comply with the law.

The following activities are carried out by third-party service providers:

- Wellington IT for the Scion system, Credit Unions software.
- Sage for payroll.
- ILCU for pension management.
- VHI for health insurance.
- Revenue for taxation and deductions.
- HR Suite for Human Resource function.
- The Irish League of Credit Unions for CU Learn and Insurance

## **Why might you share my personal data with third parties?**

We may share your personal data with third parties where required by law, where it is necessary to administer our relationship with you or where we have another legitimate interest in doing so.

## **Planned data transmission to third countries**

This credit union does not currently and does not anticipate any transmission of personal data to third countries.

~~Should this change, we will inform you of the safeguards used to allow for such processing~~

However, third parties who provide services to the credit union may be located in the UK or outside the EEA. To ensure that your personal data receives an adequate level of protection, to ensure that your personal data is treated by those third parties in a way that is consistent with and which respects the EU and UK laws on data protection, any transfer shall be made in accordance with the EU approved adequacy decisions for the EU GDPR

and the Law Enforcement Directive (LED).

### **Data Retention Periods**

We will only retain your personal data for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements.

To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

In some circumstances we may anonymise your personal data so that it can no longer be associated with you, in which case we may use such information without further **notice** to you. Once you are no longer Credit Union Personnel we will retain and securely destroy your personal data in accordance with our data retention schedule which is available on request.

### **Changes to this privacy notice**

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal data.

### **Automated decision-making**

We do not envisage that any decisions will be taken about you using automated means, however we will notify you in writing if this position changes.

### **Breach Notification**

In the unlikely event that the credit union suffers a data breach, we have an appropriate response plan in place. If your personal data has been breached and is likely to result in a high risk to your rights and freedoms, we will notify you without undue delay. We will also notify the Data Protection Commissioner within 72 hours of becoming aware of the breach. An incident report will be carried out on each breach that occurs to analyse the effects of the breach, why the breach occurred and how we can prevent it happening again.

If you have any concerns regarding data breaches in the credit union or would like to report a data breach to us, you can do so by contacting the Data Protection Officer (details above).

**If you are in receipt of information that does not concern you, please do not destroy the information but return it to our office as soon as possible.**

### **Exercising your Rights**

If you wish to exercise any of the below rights, you can download the “Rights Request Form” from [www.mylimerickcu.ie](http://www.mylimerickcu.ie) or request a copy from our office. This form has a guidance document attached which will assist you in completing your request. You can send your request by post, email or by handing it to our office. All requests should be addressed to the Data Protection Officer. Please note we may need to verify the identity of the person making the request, in which case we may ask you to provide us with a copy of your photo ID and proof of address before we can complete the request.

### **Complaints**

Limerick and District Credit Union endeavours to meet the highest standards when collecting, using, storing and destroying your personal information. We urge you to notify us if you think that our processing activities are unfair, misleading or inappropriate. We also welcome any suggestions for improving our procedures. This privacy notice aims to provide you with comprehensive detail of all aspects of our data processing; however we

are happy to provide any additional information that may be necessary. All complaints, queries or suggestions should be addressed to the DPO of the credit union.

If you have any questions about this privacy notice, please contact the DPO at the contact details set out above.

I, \_\_\_\_\_ (employee/officer/volunteer, contractors, agency workers, consultants, directors) acknowledge that on \_\_\_\_\_ (date), I received a copy of Limerick & District Credit Union's privacy notice for employees, workers and contractors and that I have read and understood it.

**Signature**

.....

**Name**

.....

<b>Your Rights in connection with your personal data are to:</b>	
	<b>To find out</b> whether we hold any of your personal data and <b>if we do to request access</b> to that data that to be furnished a copy of that data. You are also entitled to request further information about the processing.
	<b>Request correction</b> of the personal data that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you rectified.
	<b>Request erasure</b> of your personal data. This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have exercised your right to object to processing (see below).



**Object to processing** of your personal data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal data for direct marketing purposes.

**Request the restriction of processing** of your personal data. You can ask us to suspend processing personal data about you, in certain circumstances.

Where we are processing your data based solely on your consent **you have a right to withdraw that consent at any time and free of charge.**

Request that we: a) **provide you with a copy of any relevant personal data in a reusable format;** or b) **request that we transfer your relevant personal data to another controller** where it's technically feasible to do so. 'Relevant personal data is personal data that: *You have provided to us or which is generated by your use of our service. Which is processed by automated means and where the basis that we process it is on your consent or on a contract that you have entered into with us.*

You have a **right to complain** to the **Data Protection Commissioner (DPC)** in respect of any processing of your data by:

**Telephone +353 57 8684800 +353 (0)761 104 800**  
**Lo Call Number 1890 252 231**  
**E-mail [info@dataprotection.ie](mailto:info@dataprotection.ie)**

**Postal Address**  
**Data Protection Commissioner**  
**Canal House Station Road**  
**Portarlinton R32 AP23 Co. Laois**

**\*\*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 data, object to the processing of your personal data, or request that we send you a copy/a third party a copy your relevant personal data in a reusable format please contact our DPO in writing using our subject rights request form to the contact details above.

**There is no fee in using any of your above rights**, unless your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

**We may need to verify your identity if we have reasonable doubts as to who you are.** This is another appropriate security measure to ensure that personal data is not disclosed to any person who has no right to receive it.

**Ensuring our information is up to date and accurate**

We want the service provided by us to meet your expectations at all times. Please help us by telling us straightaway if there are any changes to your personal data. If you wish to avail of either of these rights, please contact us at the contact details set out above.