CUP Data Protection Privacy Notice - June 2025

Contents

Who does this Privacy Notice apply to?

As a member* of Credit Union Plus (CUP), you share your information with us. This allows us to provide our products and services to you and in doing so, we commit to protecting your information. This Data Protection Privacy Notice provides you with information about Data Protection at Credit Union Plus. ** Note: In some cases, such as loan guarantor, company director, account trustee, nomination, or an individual supporting a member's loan application, we may process third party or non-members' data. Whilst this Privacy Notice is directly addressed to members, it also applies to circumstances such as these, including references to personal data typically collected, such as name, address, data of birth and other aspects such as data security, and data retention periods.*

What is Data Protection?

If you give your personal details to an organisation or individual, they have a duty to keep these details private and safe. As the organisation who controls the contents and use of your personal details, Credit Union Plus (CUP) is the Data Controller. CUP has appointed a 'Data Protection Officer' (DPO), who is responsible for overseeing the protection of your rights in how we conduct our business, and seeking to ensure the credit union's overall compliance with Data Protection laws and regulations.

On 25 May 2018, Regulation (EU) 2016/679 of the European parliament and of the council, the General Data Protection Regulation (GDPR), came into effect. This set out a series of new EU laws concerning how data is processed and used. The objective of the regulation is to strengthen and standardise data protection laws for all EU citizens. These regulations apply to any organisation that controls and/or processes data on behalf of an individual or group of individuals. Those responsible for adhering to these regulations include employees of the organisation, as well as contractors, consultants, agents, system providers, sub-processors, and third parties who have access to data either directly or indirectly.

Data Protection at Credit Union Plus

We always understand and appreciate the trust that members, and occasionally, other parties, place in us to collect, process, and protect your personal information. As the Data Controller and processor of your personal information, we have and will continue to:

- act responsibly and give priority to the security of your information through seeking to embed a strong culture of compliance
- provide you with the assurance that your information is safe and secure through how we manage our controls, processes and systems to improve our level of customer service; and
- conduct our business in a fair and transparent way and ensure we minimise the risk or impact on your data rights and freedoms.

Who is Credit Union Plus?

Credit Union Plus provides financial and related services to our members. Our head office and main branch is in Navan and we have other branches at Ballivor, Ballyjamesduff, Clonmellon, Dunshaughlin. References in this notice to Credit Union Plus Limited (CUP) will also include "CUP" or "We" or "Us" or "Our".

Data Protection Officer

To ensure that your rights are protected, our Data Protection Officer (DPO) oversees the collection, use, sharing, and protection of your information. The DPO may be contacted by email at dpo@creditunionplus.ie, by telephone on 046-9021395, or in writing at: Data Protection Officer, Credit Union Plus, Kennedy Road, Navan, C15 TF86, Co. Meath.

How do we collect your personal information?

We collect personal information from you, when you:

− open a new account (including current account)

− lodge or withdraw monies

− apply for a loan or support a loan application (e.g., guarantor)

− apply to use our services, or

− contact us.

Information is collected through market research, our website, social media, apps, and the CCTV at our premises. Our website uses 'cookies'. This is technology used by the website to place a small text record on your PC or mobile device, when you visit our website. The cookie helps to provide a better experience for you. Please refer to our Cookie Policy for more information.

When you apply for a loan with us, we verify your identity and update our records, where required. During the loan application process and the period while you repay the loan, we also conduct information searches, and provide information to third parties, including:

- credit reference agencies
- automated loan application review system
- the Central Credit Register (www.centralcreditregister.ie/privacy/) - CRIF Realtime Ireland Limited (https://www.crif.com/privacy-policy/) - credit collection agencies.
- Open banking facility for members who opt to supply their bank statements to us directly from their bank account.

The third parties and CUP may retain the information for a period of time, whether the application proceeds to drawdown or otherwise.

What information do we collect?

To open an account, conduct business with us and/or make loan applications we collect:

- Personal Information
- Personal Financial Information
- Special Categories of Personal Data.

See Appendix 1 for full breakdown of information collected

How do we use the information that we collect?

We use your personal information for the following purposes:

- Provide and maintain our products and services to you
- Find out how we can improve our products and services
- Assess loan applications
- Credit control
- Inform you how our products and services might help you and how you can avail of them
- Protect our interests, and
- Fulfil our legal and regulatory obligations.

We need to collect and use your personal information to provide products and services to you under our terms and conditions (Ts & Cs). If you do not provide your personal information, we may not be able to provide our products and services.

Information that we collect on how you use our products and services and from our website, apps and social media is analysed by us. This helps us to know how we engage with you, how you use our products and services, for marketing information, and protection from financial crime and fraud.

We analyse information and report trends, including to third parties about loan applications, loan repayments, activity on our web-site, and activity on mobile devices. Reports and trends have the information anonymised; i.e. names and addresses are removed. Information that is shared in these reports does not include anything that would identify you or your account number. We may use technology to help automate our decision-making, for example for loan applications. Decisions are generally assessed by us using a combination of the technology, the personal information you provide to us, your information that we already hold and information from third parties. All processing of your information must be supported by a lawful basis and in that context, we fully meet our legal and regulatory obligations. We will notify you if we change the purpose for which we use your information.

What is the lawful basis to process your information?

To meet our legal and regulatory obligations we collect and retain your information by relying on one or more of the following basis:

- Your agreement and consent
- To create and maintain a contract
- A legal obligation
- Protect your vital interests and those of others
- In the public interest, and
- Our legitimate interests.

Examples of where we rely on Legitimate Interests as a lawful basis for processing include:

- To develop strategy, undertake statistical analysis, and assess current and future Credit Union financial performance;
- As part of our commitment to making informed decisions about products and services, 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 safeguard the financial stability of the credit union into the future.

  We generally 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. The only processing exception is our geo-location application, which transforms addresses into small area codes to prevent individual households from being identifiable. However, 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 on page 3 of this notice. Your trust and confidence are integral to our operations, and we are committed to addressing any concerns you may have regarding the use of your information.

See Appendix 2 for further detail on lawful basis, and how we use your information

What are our legal and regulatory obligations?

Under our regulatory and legal obligations, we are required to collect, verify and retain up to date personal information through regular checks. We are required to delete it once we no longer have to keep it. We may also gather information about you from third parties to help us meet our obligations. To process a loan application, we supply your personal information to Credit Reference Agencies (CRAs) and they give us information about you, such as about your financial history. We do this to assess creditworthiness, confirm your identity, manage your account, trace and recover debts, and prevent criminal activity.

Until such time as your loan is fully repaid, we continue to exchange information about you with CRAs, including about your settled accounts and any debts not fully repaid on time (Note: This includes loan guarantors). CRAs may share your information with other organisations. Your data may also be linked to the data of your spouse or any joint loan applicants.

Financial institutions in Ireland are required, under legislation which incorporates into Irish law the US Foreign Account Tax Compliance Act (FATCA) and the Organisation for Economic Cooperation and Development (OECD) Common Reporting Standard (CRS), to seek answers to certain questions for the purpose of identifying accounts that are reportable to Revenue for onward transmission to tax authorities in relevant jurisdictions.

Financial institutions in Ireland, including Credit Union Plus, are required to seek answers to questions regarding tax residency. If members or prospective members do not provide all of the information requested, we may not be able to proceed with opening a new account or keeping an existing account open until the relevant information is provided and we may be obliged to include the account(s) details in the annual FATCA and CRS returns to Revenue.

Under the Ireland Safe Deposit Box, Bank and Payment Accounts Register (ISBAR) regulations, the credit union is required to submit personal data including name, address, and date of birth to the Central Bank of Ireland for account holders and persons purporting to act on behalf of account holders.

Personal information collected from you is and will be shared with fraud prevention agencies who will use it to prevent fraud and money-laundering and to verify your identity. If fraud is detected, you could be refused certain services by us. If you do not provide the information we need, or help us keep it up to date, we may not be able to provide you with our products and services.

Credit searches and references

When you apply for a loan, we carry out information searches and verify your identity (Note: This also applies to prospective loan guarantors). We share your information with credit reference agencies, such as the Central Credit Register (CCR) and CRIF Realtime Ireland Ltd (CRIF). When you enter into a credit agreement with us, this data is registered on the CCR database. Each month, the CCR receives an update for each open account. This builds up a credit history which indicates how you are meeting the repayment terms of any credit agreements you may have. When you apply for a loan, we may access CCR's and CRIF's databases to obtain your credit report, and your personal data may be shared with a third party processor for this purpose (Note: This also applies to prospective loan guarantors). You may have loans from one or more credit providers. Your credit report includes details of all registered loans, open and closed. Credit agreements are retained on the CCR's and CRIF's databases for 5 years after they are closed. You may not have any credit history in the cases where you have not borrowed previously, or where any credit agreements have been concluded for more than 6 years.

Further information on the CCR and CRIF is available in their full notices on their websites, www.centralcreditregister.ie and https://www.crif.ie/.

Consent

We sometimes need your consent to use your personal data. In some cases, we may require consent from third parties such as spouse, partner, guarantor, or payee to use their personal data for processing activities such as loan applications and external transfers. If we use your sensitive personal information (or Special Categories of Personal Data as it is known in GDPR), such as medical or biometric data, we ask for your explicit consent. We ensure that you are informed when making your decision and that you are aware that you can remove your consent at any time by contacting us.

We ensure your consent is obtained under the following principles:

- **Positive Action**. Clear affirmative action by you is required. We do not use pre-ticked boxes, imply or assume consent if there is no positive action from you

- **Free will**. Your consent must be freely given and not influenced by external factors

- **Specific**. CUP will be clear on what exactly we are asking your consent for

- **Recorded**. We keep a record of your consent and how you provided it

- **Can be withdrawn at any time**. CUP stops data processing that requires your consent at any time you make a valid request. You can withdraw your consent at any time, however this may affect your ability to transact with us.

Direct marketing

We need your consent to make you aware of products and services which may be of interest to you. We may do this by telephone, post, email, text or through other digital media.

When you become a member or apply for a loan, you can decide how much direct marketing you wish to receive.

We analyse information that we collect through your use of our products and services and on our social media, apps and websites, as part of our direct marketing. This helps us understand your financial behaviour, how we interact with you and our position in a market place. This helps us to provide you with the most suitable products and services.

You may opt out at any time, including if we contact you to ask about our products and services or how they can be improved.

Keeping your information safe and secure

We protect your information with security measures under the laws that apply. We keep our computers, files and buildings secure. The collection, use, sharing, protection and deletion of your information is overseen by our Data Protection Officer (DPO). Our DPO advises on how we can best understand risks to your data rights and freedoms and processes implemented to protect these. The DPO has responsibility to report to the Office of the Data Protection Commissioner if there is any breach of your data or our obligations.

When you contact us to ask about your information, we may require you to identify yourself – this is to help us protect your information.

To meet our legal and regulatory obligations, we hold your information while you are a member and for a period of time after that, in line our policy requirements, which generally align with legislative requirements. The table in Appendix 3 will help you understand how long we hold some of your data for. We hold all data while you are an active member with us.

While these retention periods are our policy, they are also subject to legal, regulatory and business requirements, which may require us to hold the information for a longer period. This includes meeting minimum retention standards for our Anti Money Laundering requirements. External authorities may also require us to retain data for longer than our policy. We must do this to protect the interests of both ourselves and members. We continuously assess and delete data to ensure it not held for longer than necessary.

See Appendix 3 for retention period detail.

Sharing your information with third parties

Sometimes, we share your information with third parties, in order to:

- provide products, services and information
- analyse information
- research your experiences dealing with us
- collect debts
- prevent financial crime
- protect both our interests.

The third parties we share information with can include:

- Credit reference agencies including the CRIF (http://www.crif.ie)
- Central Credit Register (https://www.centralcreditregister.ie)

− Fraud prevention agencies

− Company search databases

− Regulatory bodies, including the Data Protection Commission (DPC) and the Central Bank of Ireland (CBI)

− Companies we have a joint venture or agreement to work with

− Insurance companies

− Government bodies, including Revenue Commissioners

− Cards/transaction processing banks

− Market research companies

− Debt collection agencies

− Automated Loan Decisioning processors

− External consultancy firms including Legal, Accountancy, Compliance and other Professional Services

- Transaction facilitators

− Any entity you request your data to be shared with.

We have contracts with third parties who provide sufficient guarantees that the necessary safeguards and controls have been implemented to ensure protection of your personal information. We also must share information with third parties to meet any applicable laws, regulations or to meet lawful requests. When we believe we have been given false or misleading information, or we suspect criminal activity, we must record this and inform law enforcement agencies.

Ways in which we may share personal data include:

- To engage professional services of third parties, who provide specialised services to us under contract, any such parties are bound by confidentiality.
    - We engage third party providers to assist with our common bond analysis. No analytics are carried out on data where individuals are identifiable. Our providers may in-turn share this data with the Irish League of Credit Unions (ILCU) to facilitate the compilation of accurate statistical information of the overall Credit Union sector.

    - This data is used by the ILCU for national and regional analysis as well as in providing valuable sectoral information which could be used for advocacy purposes, such as when engaging with government on behalf of credit unions.

Transfers of personal information outside of the European Economic Area (EEA)

Some service providers that we may share your personal information with may be located in a country that does not have data protection laws which provide the same level of protection as the laws in Ireland. Some countries already have adequate protection for personal information under their applicable laws. In other countries safeguards will be applied to maintain the same level of protection as the country in which the products and services are supplied. These safeguards may be contractual agreements with the overseas recipient or it may require the recipient to subscribe to international data protection frameworks. For more information about the European Commission's decisions on the adequacy of the protection of personal information in countries outside the EEA, please visit: https://ec.europa.eu/info/law/law-topic/data-protection_en.

We may transfer your personal information to the UK, under the Adequacy Decision between the EU and the UK agreed under Article 45 of the GDPR.

If you are registered to use our online account/banking platform cu Online +, Wellington Computer Systems Limited (which hosts our platform) will also be a controller of your personal data. To help you understand what it does with your personal data, and how to exercise your rights in respect of their processing of your personal data, you should review its privacy policy: https://www.well-it.com/privacy-policy

If we issue you a debit card, Transact Payments Malta Limited (which is an authorised e-money institution) will also be a controller of your personal data. To help you understand what it does with your personal data, and how to exercise your rights in respect of their processing of your personal data, you should review its privacy policy: http://currentaccount.ie/files/tpl-privacypolicy.pdf

Your rights to your personal information

If you wish to exercise your personal information rights, please contact the Data Protection Officer (see contact details on Page 3).

When you contact us to ask about your information, we may ask you to identify yourself. This is to help us protect your information. You have the right to obtain information, however this right cannot affect the rights and freedoms of others. We cannot therefore provide information on or about other people without their consent.

We will provide your information without charge. As permitted under the regulations however, where information requests are manifestly unfounded or excessive, we may either charge a reasonable fee or refuse to act on the request. Your rights are detailed more fully in the next section.

Access your personal information

You can request a copy of the personal information we hold and further details about how we collect, share and use your personal information. You can request the following information:

− the information we hold on you

− the purposes of the processing

− the categories of personal data concerned

− the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations

− where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period

− where the personal data are not collected from you, any available information as to their source

− the existence of automated decision-making and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for you.

Updating your personal information

You may update or correct any of your personal details. Please contact us at 046-9021395 or call to any of our branches. Please ensure that key updates such as address or name (e.g., spouse's surname) are notified as soon as possible.

Removing your consent

If you have given us consent in relation to the use of your personal information, you can change your mind and withdraw your consent. This could be for direct marketing or processing your sensitive (Special Categories of Personal Data) information, such as medical or biometric data. Please contact us at 046-9021395 or call to any of our branches.

Restricting and objecting to processing your personal information

You may have the right to restrict or object to us processing your personal information. We will require your consent to further process this information once restricted. You can request restriction of processing where;

− The personal data is inaccurate and you request restriction while we verify the accuracy

− The processing of your personal data is unlawful

− You oppose the erasure of the data, requesting restriction of processing instead

− You require the data for the establishment, exercise or defence of legal claims but we no longer require the data for processing

− You disagree with the legitimate interest legal basis and processing is restricted until the legitimate basis is verified.

Deleting your personal information (your right to be forgotten)

You may ask us to delete your personal information or we may delete your personal information if:

− the personal data are no longer necessary in relation to the purposes for which they were collected or processed

− you withdraw your consent where there is no other legal ground for the processing

− you withdraw your consent for direct marketing purposes

− you withdraw your consent for processing a child's data

− you object to automated decision making

− the personal data have been unlawfully processed

− the personal data have to be erased for compliance with a legal obligation.

Moving your personal information (your right to data portability)

If you request and where possible, we can share a digital copy of your information directly with you or another organisation, we will provide this information in a 'structured, commonly used and machine-readable format'. We can only share this information where it has been processed automatically (hard copy documents are excluded for portability) and was processed under your consent or performance of a contract. We do not share information processed under legal obligation or our legitimate interest for portability – this is in line with GDPR guidance.

Right to lodge a complaint with a 'Supervisory Authority'

If you have a complaint about your personal data or any related matter, please contact us on 0469021395, or contact a member of staff in any of our branches. If corrections are required, our staff will prioritise and attempt to make these as quickly as possible. If issues are not suitably, promptly, or satisfactorily addressed, you may also make a complaint to the Data Protection Officer (see page 3 for contact details). Any complaint you make to us will be investigated as fully as possible. Please provide as much information as you can to help us quickly and satisfactorily resolve your complaint. You may also contact the Office of the Data Protection Commission via their web-site www.dataprotection.ie, by email at info@dataprotection.ie, or by post at: Office of the Data Protection Commissioner, Canal House, Station Road, Portarlington, R32 AP23, Co. Laois.

Automated decision-making

We may use technology to help us make decisions that are as efficient, quick, and fair as possible. This is generally based on the provided directly by you, information we may hold about you, and information from third parties. For example, when you apply for credit with us, we use different data sources to understand and assess your ability to repay the loan. This helps ensure responsible lending.

We use the information provided by you on the applications and information from third parties such as credit reference agencies. The information we may process as part of automated reviews includes:

- Name
- Date of Birth
- PPSN
- Phone number
- Email address
- Residential/business address
- Income
- Financial position
- Transaction history
- Employment details
- Discretionary spending
- Credit rating
- Your other loans, mortgages and products
- Bill repayments

Analysing this information helps us assess ability to repay and meet the periodic loan payments. The automated system output and/or recommended action is just one component of our overall decision making process with regard to credit decisions.

Our current provider's data protection policy is at:
https://www.graphicalfinancialanalysis.com/Policies/PrivacyPolicy.pdf

Updates to this notice

From time to time, we will update this notice if we change how we use your information, change our technology or change our products. The most up to date notice is always on our web-site, www.creditunionplus.ie

Glossary of terms used in this notice

This glossary is provided to assist your understanding of the data protection terms in this notice. *Anonymisation*: process of turning data into a form which does not identify individuals and where identification is not likely to take place. The data once anonymised will no longer be personal data. The intention of anonymisation is that the data is irreversibly changed.

Automated Data: Information on computer or information recorded with the intention of or the ability of putting it on a computer. It includes information in any electronic format.

Automated Decision-Making (ADM): when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. Automated Processing: any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's economic situation.

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 or dactyloscopic (finger print) data. Consent: of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Data: means individual facts, statistics, or items of information regarding an individual. Data can refer to automated data and manual data.

Data Controller: means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by EU or Member State law, the controller or the specific criteria for its nomination may be provided for by EU or Member State law.

Data Subject: means an identified or identifiable natural person (see Personal Data). Data Processor: A Data Processor is a person who processes personal data on behalf of a data controller but does not include an employee of a data controller who processes such data in the course of his/her employment.

Data Protection Officer (DPO): the person required to be appointed in specific circumstances under the regulations. The DPO oversees how we collect, use, share, and protect information.

EEA: the 28 countries in the EU, and Iceland, Liechtenstein and Norway.

Explicit Consent: consent which requires a very clear and specific statement on the part of the Data Subject.

General Data Protection Regulation (GDPR): the General Data Protection Regulation ((EU) 2016/679). Personal Data is subject to the legal safeguards specified in the GDPR.

Information and Records Management: the application of systematic policies and procedures governing the creation, distribution, maintenance, management, use and ultimate retention or disposal of records to achieve effective legal, economical, accountable, transparent and efficient administration.

Lawful basis: the processing of data must be performed under a lawful basis. Personal data may be processed:

- On the basis that the data subject has provided consent to do so
- On the basis that it is necessary in order to enter into or perform a contract
- On the basis that there is a legal obligation for the processing
- Where Credit Union Plus has a legitimate interest in processing the data
- In order to protect the vital interests of the data subject
- In the public interest.

Personal Data: means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Processing or Process: means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Records: documents in every format created and received by individuals or organisations in the course of conduct of affairs and accumulated as evidence of these activities.

Relevant Filing System: Is any set of information that, while not computerised, is structured by reference to individuals, or by reference to criteria relating to individuals, so that specific information is accessible.

Special Categories of Personal Data: information revealing:

- Personal data revealing racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data and biometric data processed for the purpose of uniquely identifying a natural person
- Data concerning health
- Data concerning a natural person's sex life or sexual orientation.

Supervisory Authority: the national independent authority responsible for upholding the fundamental right of individuals in the EU to have their personal data protected. The Office of the Data Protection Commissioner (ODPC) is the Irish supervisory authority for the General Data Protection Regulation (GDPR). It also has functions and powers related to the Irish ePrivacy Regulations (2011) and the EU Law Enforcement Directive.

Appendix 1 – Primary Information collected

Personal Information	Personal Financial Information	Special Categories of Personal Data*
Full Name	Personal bank and credit card account details	Health data: required for loan protection insurance
Signature	Income and expenditure	Your financial transactions may reveal "Special Categories of Personal Data", such as political opinions or religious beliefs. This can occur if your bank statements show transactions, for example, donating to political parties, organisations, churches or parishes
Date of Birth	Statement of net worth	
Home/Business address	Transactions, purchasing and spending activity	
Email address	Revenue documents e.g., P60, Form 11	
Phone number(s)	Payment instructions	
Gender	Account positions and history	
Marital status	Credit records, worthiness, standing or capacity	
Partner and dependents	Business accounts and expected turnover	
Proof of identity including driving license, passport, birth certificate	Origin/source of funds	
Proof of address including bank statements and utility bills	Purpose of account(s)	
Tax Identification Number		
Personal Public Service Number (PPSN)		
Educational details		
Mother's maiden name		
IP address		
Profession/Job		
CCTV images		
External Payee details	Payee Details, Name, bank details	

* Under the GDPR, 'Sensitive Personal Information' is known as 'Special Categories of Personal Data' and requires additional safeguards for processing

Appendix 2 – Lawful basis, and how we use your information

Lawful Basis	How we use your information
Your agreement and consent: We require your consent to process certain information such as Special Categories of Personal Data. We ensure your consent is obtained under the following principles: − Positive Action. Clear affirmative action by you is required. We do not use pre-ticked boxes, imply or assume consent if there is no positive action from you − Free will. Your consent must be freely given and not influenced by external factors − Specific. We will be clear on what exactly we are asking your consent for − Recorded. We will keep a record of your consent and how we got it − Can be withdrawn at any time. We will stop data processing that requires your consent at any time you make a valid request. You can withdraw your consent at any time **Special Categories of Personal Data** is information relating to: − Racial or ethical origin, political opinions or religious or philosophical beliefs − Trade union membership − Biometric data − Genetic data − Physical or mental health − Sexual life/orientation − Commission or alleged commission of any offence by the data subject, or − Any proceedings for any offence committed or alleged	To directly contact you about our products and services: With your consent, we will let you know what products or services you might like. You can select how you prefer to be contacted on our application forms or by contacting us. **To process Special Categories of Personal Data**: - We only process Health Data, which is required to assess loan protection insurance. Your explicit consent will always be obtained before the collection and processing of Health Data.
To create and maintain a contract: We collect and process your information to allow us to provide products and services to you	**Providing products and services.** We provide accounts, loans, online and mobile services. Your information is processed to validate your use of these products and services. **Maintain products and services.** We monitor and update information to ensure that it is up to date and accurate. We may share the information with third parties. **Repayment of loans and collect outstanding debts.** We monitor all loans and their repayments. When repayments are overdue we may share information with and engage third parties

Lawful Basis	How we use your information
Legal obligation: In our day to day business and in our dealings with members, we must comply with all laws and regulations	**Identify and validate our membership.** We are required to collect and process certain personal information to validate your identity. We share this information with third parties for validation and legal purposes
Protect your vital interests and those of others	**We share information to protect you.** Occasionally, we could suspect that you and other members of the Credit Union may become victims of financial fraud. If this arises, we will share information with third parties to help prevent fraud and keep you protected.
In the public interest	**Prevention of fraud and financial crime.** We may suspect that you or other Credit Union members may become victim of a financial fraud or identify activity that may lead to a financial crime. We will share information with third parties to help prevent fraud and financial crime.
Our legitimate interests: CUP exists to provide savings and loans to our members. Our legitimate interests are to ensure that we provide you with the products and services that you need, manage the business efficiently and comply with all laws and regulations.	**Manage the Credit Union on behalf of members.** We review how our products and services are used to keep them up to date. We ensure that all data is held safely and securely by us with appropriate computer safeguards in place. We review and mitigate all known risks to maintain the most secure systems and procedures. We regularly produce internal management and Board reports to assess how we run the business and develop our strategies. We share information with third parties to help manage these risks and protect both our interests. This includes Know Your Customer, Anti-Money Laundering and Credit Referencing checks. To allow you to become a member and to offer loan products we musty validate your identity and your ability to repay a loan. We may share information with third parties to conduct checks and validate our information. **Conduct research with our members.** We regularly review our products and services and the satisfaction of our members. We do this by collecting and analysing data to better inform us and help us the efficiently run the business.

Lawful Basis	How we use your information
	We may also share this data with third parties who assist us with research. All personal information is removed before the data is shared. **Improve our products and services.** By collecting and analysing data, we can identify groups of members and trends in the wider market. Using the analysis described we enhance our products and services to continuously meet your needs. This can also allow us to provide a more personalised member service. **Prevent financial crime and protect our computer network and data.** We continually monitor and analyse activity on our computer network to identify any possible financial crime threats and protect the data. **Know Your Customer, Anti-Money Laundering and Credit Referencing checks.** To allow you to become and/or remain a member including offering loan products, we must validate your identity and your ability to repay a loan. We may share information with third parties to conduct checks and validate our information.

*Appendix 3 - Retention period**

Service/Document Type	Document	Retention Period
Membership Application and Account Opening	− Account Opening documents −Legal / Regulation Identification Documents − Account Records − Member Information − Member Complaints − Member Instructions − Member Communications − Deceased Accounts − Loan Protection / Life Savings (LPLS) Insurance Claims − Security Information − DIRT Information − Nomination Forms − Other Correspondence	7 years after account is closed
Credit Applications, Credit Approvals and Credit Control	− Credit Assessments − Credit Approvals − Credit Agreement − Credit Agreement Variations (e.g. Loan Reschedules) − Credit Control	7 years after loan repayments completed or replaced when new loan approved
Transactions (i)	− Lodgement and Withdrawal − Saving documentation − IP address of payment instruction device	7-10 years after the transaction**
Transactions (ii)	− Standing Order, Direct Debit and EFT mandates	7 years after account is closed
Other	− Health & Safety Reports − Legal Reports	10 years

*These may be subject to change, primarily due to various updates to our legislative and regulatory requirements.

** SEPA Instant payment providers may retain personal data, financial data, and IP address for 10 years, in compliance with their various legal, regulatory and contractual obligations.