Data Protection Policy

Contents

1. Objective of Policy

This Data Protection policy is a statement whereby we at Cairde Credit Union commit to protecting the rights and privacy of individuals in accordance with the Data Protection Act, 2018 (the Act) requirements and the General Data Protection Regulation 2016/679 (GDPR). It ensures that Cairde Credit Union:

- Is compliant with the relevant data protection legislation and follows what is considered industry good practice in protecting the personal data collected, stored, and processed;
- Protects the rights of our staff, members, volunteers, directors, volunteers and partners as they relate to data protection and privacy;
- Is open and transparent in relation to how we collect, store and process individuals' personal data; and
- Protects the organisation from the risks of a data breach.

The policy covers both personal and special categories of personal data held in relation to data subjects by Cairde Credit Union as defined by the Act and GDPR. The policy applies equally to personal data held in both manual and automated forms. All personal data and special categories of personal data will be treated with equal care by Cairde Credit Union. Both categories will be equally referred to as Personal Data in this policy, unless specifically stated otherwise.

At Cairde Credit Union we need to collect and use certain personal information from the following persons:

- Credit Union Members
- Employees
- Officers
- Volunteers of the Credit Union
- Suppliers
- Business Contacts

These guidelines set out the requirements of the Act and GDPR and the steps to be taken by us when processing personal data. These guidelines will be updated, as required, to allow for any legislative changes.

These guidelines apply to all staff of the Credit Union including permanent and temporary staff, volunteers and any other parties who are authorised to access Personal Data held by the Credit Union.

Data Protection law safeguards the privacy rights of individuals in relation to the processing of their personal data. The Act and GDPR. confers rights on individuals as well as responsibilities on those persons processing personal data. Personal data is data relating to a living individual who is or who can be identified, either from the data or from the data in conjunction with other information available.

2. Policy Compliance Statement

This policy is in compliance with the following:

- The General Data Protection Regulation 2016/679 ("GDPR")
- The Data Protection Act 2018 ("the Act")
- The Credit Union Act, 1977 (as amended)

We may update our Privacy Policy from time to time. Our current Privacy Policy will always be available to download from our website www.cairdecu.ie.

If we make any material changes to our Privacy Policy, we may also contact you by other means to inform you of the changes taking effect, such as by phone, email, post or posting a notification on our website.

3. Roles and Responsibility

Board of Directors:

The Board of Directors has overall responsibility for ensuring compliance with the Data Protection legislation. The Board of Directors will approve, review and update the Data Protection Policy at least annually.

Management / CEO:

The Management / CEO will ensure that the Data Protection Policy is implemented and ensure controls are in place to facilitate compliance in line with the guidance of the Data Protection Officer (DPO).

Staff:

All employees of the Credit Union who collect and / or control the contents and use of personal data are responsible for compliance with the Data Protection Policy.

The Data Protection Officer (DPO):

The DPO will undertake a number of tasks that will include, but not necessarily be limited to the following:

- Inform, advise and issue recommendations to the organisation regarding compliance with data protection requirements;
- Asist in fostering a data protection culture within the organisation and help to implement essential elements of all relevant data protection and privacy regulations and legislation.
- Create and implement policies and procedures in relation to data processing, data subjects' rights, data protection by design and by default, records of processing activities, security of processing, and notification and communication of data breaches.
- Advise the controller / processor regarding:
    - Whether or not to carry out a data protection impact assessment

  - What methodology to follow and appropriate resource when carrying out a DPIA.
  - Whether or not the DPIA has been correctly carried out and whether its conclusions (whether or not to go ahead with the processing and what safeguards to apply) are in compliance with data protection and privacy requirements.
  - What safeguards (including technical and organisational measures) to apply to mitigate any risks to the rights and interests of the data subjects.
- Provide oversight the record of processing operations under the responsibility of the controller as one of the tools enabling compliance monitoring, informing and advising the controller or the processor;
- Document all decisions taken consistent with and contrary to advice given; and
- Offer consultation once a data breach or other incident has occurred.

4. Data Protection Principles

Cairde Credit Union undertakes to perform our responsibilities under the regulation, as follows:

- Personal data shall be collected and processed lawfully, fairly and in a transparent manner in relation to the data subject (**'lawfulness, fairness and transparency'**);
- Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with the Act and GDPR, not be considered to be incompatible with the initial purposes (**'purpose limitation'**);
- Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (**'data minimisation'**);
- Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (**'accuracy'**);
- Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with the Act and GDPR subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (**'storage limitation'**);
- Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (**'integrity and confidentiality'**)

- The Data Controller (Cairde Credit Union) shall be responsible for, and be able to demonstrate compliance with, the above listed principles (**'accountability'**).

5. Rights of the Data Subjects

Cairde Credit Union will also endeavour to uphold the rights of data subjects as laid out in the Act and GDPR as follows:

- Provide transparent information and communication to data subjects on how to exercise their rights;
- Provide information about our processing activities to the data subject;
- Provide the data subject with the right to obtain from us confirmation as to whether or not we are processing personal data concerning him or her and, where that is the case, access to the personal data;
- Provide the right of rectification for the data subject to correct inaccurate personal data concerning him or her;
- Provide the data subject with the right to obtain from us the erasure of personal data concerning him or her without undue delay and we shall have the obligation to erase personal data without undue delay unless we have overriding legitimate grounds for continued processing. This will be handled on a case by case basis under the circumstances listed in the Act and GDPR;
- Allow the data subject to restrict the processing of their data unless we have an overriding legitimate lawful purpose for continuing to process the data;
- Provide the data subject with the right to receive the personal data concerning him or her, which he or she has provided to us, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller under the conditions listed in the Act and GDPR; and
- The data subject shall have the right to object to processing concerning them and to have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

Please note that the above rights are not always absolute and there may be some limitations.

6. Key Definitions

Cairde Credit Union collects and maintains Personal Data on our members and are therefore subject to the provisions of the Act and GDPR as a Data Controller. Personal Data includes automated data (e.g. information held on computer systems) as well as manual data (e.g. paper based filing systems).

The Key definitions are set out in the Act and GDPR. are summarised below.

The term "**personal data**" is information related to a living individual who is or who can be identified:

a) from the data, or

b) from the data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

The term "**special categories of personal data**" means personal data revealing:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetic data;
- biometric data for the purposes of uniquely identifying a natural person;
- any form of health information; and
- a natural person's sex life or sexual orientation.

Data "**processing**" includes obtaining, recording or holding information and carrying out any operation on the information such as organising, altering, using, disclosing, erasing or destroying it.

A "**data subject**" is an individual who is the subject of personal data. This includes partnerships and groups of individuals, but not limited companies. In terms of Cairde Credit Union, all Credit Union members, employees, officers and volunteers are data subjects.

A "**data controller**" means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

A "**data processor**" means any person (other than an employee of Cairde Credit Union who processes the data on behalf of Cairde Credit Union.

"**Consent**" 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.

7. Implementation, Management, Monitoring and Review

Implementation

Implementation of this Policy is the responsibility of the Credit Union management. In addition, management are responsible for the development and maintenance of a data retention schedule in respect of any paper-based data or system handling personal data. Details of retention are contained in the Records Management Policy.

Management

Management are responsible for ensuring that all staff, officers, volunteers and any other parties working on behalf of the Credit Union observe the provisions of this policy.

While not all staff members will be expected to be experts in data protection legislation the Credit Union is committed to ensuring that staff have sufficient awareness of the legislation to be able to anticipate and identify a data protection issue, should one arise. In such circumstances, staff must ensure that the CEO is informed in order that appropriate corrective action is taken.

This policy provides the top-level guidelines for the handling of all data. The Credit Union is firmly committed to ensuring personal privacy and compliance with relevant data protection legislation, including the provision of best practice guidelines and procedures in relation to all aspects of data protection and to support this policy.

In general terms, our staff are informed that they should always consult with their manager or the DPO to seek clarification on any data protection matters.

Monitoring

Compliance with this Policy will be monitored by the DPO and management. If anyone considers that this Policy is not being followed, they should raise the matter with their manager or the DPO.

Review

This policy is, at a minimum, reviewed annually by the Board of Directors and as soon as is practically possible following any new regulation or legislation that may impact upon the data protection requirements of the Credit Union.

8. Types of Personal Data Held

Cairde Credit Union collects and uses Personal Data such as the following:

- General: name, address, date of birth, email, telephone numbers, photo;
- Financial data: bank account details, financial status and history, banking details and transactions, borrowings, debit card details and receipts;
- Contract data: details of the credit union products member hold with us, signatures, identification documents, salary, occupation, payslips, source of wealth, source of funds, Politically Exposed Status, accommodation status, mortgage details, previous addresses, spouse, partners, nominations, Tax Identification/PPS numbers, passport details, driver license details, tax residency, beneficial owners information, medical information, tax clearance access number, parent/guardian information (for minor accounts)
- Data collected through interactions with credit union staff and officers: CCTV footage, telephone voice recordings, email correspondence, records of current or past complaints,
- Other data: photo or videos of prize winners, IP addresses, tracking information from cookies.
- Special Category Data: Health data relevant to the provision of insurance, biometric data if a member joins our credit union through our App.

In certain instances, an individual may supply us with information relating to another individual. This may occur in the following cases:

- Bank statements provided where the account is in joint names,

- Utility bills in joint names
- Personal information contained in sets of Business Accounts

In these instances, it is the responsibility of the individual providing the data to ensure the other named individual/s are aware their data is being shared and do not object to this.

9. Purposes for Processing Personal Data

Account Opening:

Cairde Credit Union 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 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 any product or service held at the Credit Union or to provide details of other services, products, offers or competitions that may be of interest to our members.

Loans: Applications, Administration and Arrears:

Cairde Credit Union 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 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 complete a submission 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;

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

The credit union will use personal data to assist it in carrying out the following:

- To record telephone conversations to offer individuals additional security, 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;
- When we issue a debit card and for the administration of a current account held in our Credit Union;
- 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;
- Apply for membership of the credit union; and
- Upload documentation required a membership stage.

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 Cairde Credit Union 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 you opt to join our credit union via our Mobile App, you will be asked to consent to the use of biometric data to carryout automated facial verification;
- 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.

10. Data Sharing and Data Transfers

We do not sell any personal information, nor do we share it with unaffiliated third parties unless we are required to do so by law. 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 enforce certain reporting, compliance and auditing on Credit Unions. We are obliged, further to Central Bank 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;
  - Government Departments such as Department of Finance and the Department of Social Protection may require the Credit Union 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;
- 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;
- to offer debit card services to our members, we have partnered with PAYAC who act as Appointed Coordinators and Programme Managers;
- We reserve the right to report to law enforcement any activities that we, in good faith, believe to be illegal;
- If we issue you with a debit card, Transact Payments Malta Limited (which is an authorised e-money institution) will also be a controller of your personal data. In order for you to understand what they do with your personal data, and how to exercise your rights in respect of their processing of your personal data, you should review their Privacy Policy which is available here http://currentaccount.ie/files/tpl-privacy-policy.pdf
- With any relevant, authorised third parties as part of a merger or acquisition, any such parties will be bound by a duty of confidentiality;
- 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.

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; or
- with companies located in a third country approved by the European Commission under an adequacy decision.

Where any of our supplier 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. Currently there is one such sub-processor (DocuSign) located outside the EEA but appropriate measures and contractual agreements are in place to protect your data in this regard.

11. Lawful Basis for Processing Personal Data

Cairde Credit Union is obligated to define a lawful basis for processing personal data. Below is a summary of our use of personal data and the lawful basis we rely on for the processing different categories of data for different purposes.

- Article 6.1(b) "*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 setup and manage accounts and provide all 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 the credit union;
- 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 apply for and obtain a debit card and to administer a current account;
- 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) "*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 2018, 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) "*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, the credit union also utilises credit data from credit referencing agencies. Our legitimate interest: The credit union, for its own benefit and therefore the benefit of its members, must lend responsibly and will use credit scoring information in order to determine suitability for a loan;
  - when carrying out searches relating to credit worthiness. Our legitimate interest: The credit union, for its own benefit and therefore the benefit of its 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 the credit union 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;
- carrying out debt collection activities in the event of non-payment of a loan or missed payments. Our legitimate interest: we have a duty to our members to ensure the financial stability of the credit union so we must collect all amounts owed to us;
- carrying out 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 to guarantee financial stability into the future. Data will always be analysed in a collated format, individual accounts will not be analysed.

- Article 6.1(a) "*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 and Research**: to provide our members with details on our products and services provided they have not opted out of receiving such communications and to carry our market research. Individuals can opt-out of receiving marketing communications at any time;
  - **Identification:** we request a member's consent to take a photo to store electronically on our database for the purpose of identification for their protection;
  - **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.
  - **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;
  - **Schools Quiz:** we participate in the Schools Quiz in liaison with the ILCU. The Schools Quiz is open to entrants aged 4 to 13. We will pass on a form to the contact in the school who is then responsible for asking the entrants' parent/legal guardians for their consent to the processing of their child's personal data. This information is processed only where consent has been given;

- Article 6.1(e) *"processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;"*
  Examples of where this lawful basis is applicable include the following:

- to combat the spread of Covid-19 in line with guidance from Public Health Authorities and Government,
- to protect our staff, members, volunteers, visitors and the wider public during the Covid-19 pandemic

12. Subject Access Requests (SARs)

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 must 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.

A Subject Access Request Form is available on our website www.cairdecu.ie. Individuals are asked to complete this form when making a SAR, 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.

Cairde Credit Union has an internal procedure in place to handle all SARs.

13. Security of Personal Data

Cairde Credit Union ensures the confidentiality, integrity, availability, and resilience of personal data when in use, transit and storage. We are obliged to protect the data from inadvertent destruction, amendment, loss, disclosure, corruption or unlawful processing.

- Appropriate security controls, including technical and non-technical are utilised to protect Cairde Credit Union personal data;
- Computer screens, printouts, files or documents displaying personal data are only visible to authorised personnel;
- Personal data held in manual (paper) files is held securely in locked cabinets, locked rooms or rooms with restricted access;
- Data printouts are shredded and disposed of securely when no longer required;

- Staff are instructed to always keep information strictly confidential and not to disclose or discuss an employee's or customer's information or circumstances with any unauthorised outside parties;
- We regularly test our systems to ensure that there are no security flaws, this includes
- Our IT partners ensure that our systems are protected and that backups are done in real time and stored securely;
- Staff and volunteers are given regular training on how best to protect the personal data they handle during the course of their work;
- Any third parties who process personal data on our behalf are contractually bound to process personal data in line with current data protection law practices and principles thus ensuring the security of the data;

The Board of Directors are ultimately responsible for ensuring that Cairde Credit Union meets its legal obligations and abides by its own policies and procedures. The company's Data Protection Officer (DPO) is responsible for handling any Data Protection queries from staff/volunteers as well as ensuring any new staff are aware of their responsibilities and for promoting awareness of Data Protection within the company.

14. Data Retention

We will only retain your 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, your personal information will be retained for 7 years from the date your credit union account closed. Where you 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.

15. Privacy by Design and Default

The regulation requires that all Cairde Credit Union systems and processes are compliant in nature. In Cairde Credit Union the use of Data Protection Impact Assessments (DPIA) will be conducted on any new project that involves the collection of personal data or special categories of personal data as well as any changes to existing projects where there are risks to the data.

The DPO should be notified in the advance planning stages of any proposed new processes or technologies or changes to existing processes. This includes internal projects, product development, software development, IT systems, and any other type of processing where personal data is affected. This will ensure that any required DPIAs can be carried out and the findings reported to the Board where necessary prior to any action being taken.

16. Notification of Data Breaches

Article 4(12) GDPR defines a 'personal data breach' as:

"*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*"

Staff at Cairde Credit Union are trained to recognise a breach and are instructed to inform their line manager immediately if they suspect a breach has occurred or have evidence of a potential breach. The line manager will then escalate it to senior management and the DPO as required.

Cairde Credit Union has a Personal Data Breach Procedure in place which will be followed by the DPO and relevant staff members in the event of a breach being reported either internally or from a third-party processor.

17. Data Protection Officer (DPO)

The role of the Data Protection Officer has been outsourced to O'Dwyer Power under a contract outlining the tasks of the DPO in assisting Cairde Credit Union in complying with data protection legislation. The tasks of the DPO are in keeping with those defined in Article 39 of the GDPR.

The Board of Directors of Cairde Credit Union are ultimately responsible for able to demonstrate compliance with the law. Management are responsible for ensuring that all personnel are trained in their obligations.

18. Data Protection and Covid-19

In order to ensure that we comply with the Public Health guidelines about what businesses must do to play their part in containing the spread of Covid-19, we may be obliged to process certain special categories of data such as health data. Other additional details may be sought including; travel information, details of close contacts and other relevant information.

The collection of data in relation to managing our response to the Covid-19 pandemic, is carried out on the lawful basis of Article 9(2)(i) GDPR Section 53 of the Data Protection Act 2018 which states:

> *"processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy"*

Also, Recital 46 GDPR states:

> *"Some types of processing may serve both important grounds of public interest and the vital interests of the data subject as for instance when processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread"*

Due to the current global Covid-19 pandemic, the processing of sensitive categories of data on this basis is justified. During this uncertain time, another consideration for the credit union is its obligations

to protect its staff under the Safety, Health and Welfare at Work Act 2005 (as amended). The responsibilities of employers outlined in this Act, together with the lawful basis stated above (Article 9(2)(i) GDPR), provide a clear basis for processing data, including health data, of staff where it is deemed necessary and proportionate to do so.

Certain data may be shared with Public Authorities when we are required to do this and data collected in relation to Covid-19 will be retained for a period of no longer than 28 days.

19. Contact Details

If you have any questions, concerns or suggestions related to our Privacy Policy, you can contact us using our details below:

Data Protection Officer, Cairde Credit Union, 3 – 6 Parnell Street, Dungarvan, Co. Waterford.
Email: dpo@cairdecu.ie Tel: 058 44088

You have a right to complain to the Data Protection Commissioner (DPC) in respect of any processing by using the details below (or completing a webform by going to: https://www.dataprotection.ie):

Data Protection Commission, 21 Fitzwilliam Square South, Dublin 2, D02 RD28.
Tel: 0578 684 800