DATA PROTECTION POLICY

This policy was adopted by the Board of Directors of Ballymena Causeway Credit Union on 17th August 2023

Ballymena Causeway Credit Union Limited
19 – 21 William St, Ballymena BT43 6AW

Contents

DOCUMENT CONTROL

Version	Date of board approval	Reviewed by	Amendments	Date of next review
Original Policy	17 February 2009			July 2011
Version 2	July 2011			July 2013
Version 3	October 2012			October 2013
Version 4	February 2014			February 2015
Version 5	August 2015			August 2016
Version 6	July 2017			May 2018 (To take account of GDPR)
Version 7	May 2018	Risk and Compliance Manager	Policy re-write in light of GDPR requirements	May 2019
Version 7.1	August 2018	Risk and Compliance Manager	S2 amendment to include reasoning for not appointing a formal DPO	May 2019
Version 8	September 2019	Risk and Compliance Manager / Data Protection Representative	S2 Deletion of staff names and insertion of staff roles S12.1.6 Deletion of "Management System (ISMS) and insertion of "Policy" Appendix 2 Insertion of reference to Account Opening Privacy Notice (Minor Accounts)	September 2020
Version 9	September 2020	Risk and Compliance Manager / Data Protection Representative	S1 Reference made to new trading name S2 Reference to Operations Manager amended to Head of Operations to reflect role title change S6 Reference made to Causeway Office S17 Operations Manager deleted and replaced by Senior Management Team	September 2021
Version 10	September 2021	Risk and Compliance Manager / Data Protection Representative	Amendment of GDPR to UK GDPR throughout. Following Brexit, the provisions of the EU GDPR have been incorporated directly into UK law as the UK GDPR. This necessitates that data protection policies will have to be separate between the jurisdictions given the potential for divergence between the two. Removal of European Commission and insertion of UK Government Removal of EEA Definition and inserted UK GDPR Definition Head of Operations replaced by Risk and Compliance Officer for Deputy DPR Role	September 2022
Version 11	August 2022	Risk and Compliance Manager / Data Protection Representative	Deletion of "EU or Member" from Footnote 4 – Brexit Related Section2 Deletion of "Risk and Compliance Officer" and insertion of "Head of Operations" as Deputy Data Protection Representative. Rationale – no Risk	August 2023

			and Compliance Officer role in place at present Insertion of new Paragraph 20 - Automated Processing (including Profiling) and Automated Decision Making (ADM)	
V12	August 2023	Risk and Compliance Manager/Data protection officer	Removal section 6 Reference to Lisnamanagh Park Removal Policy review date – Section 22 Section13 'RCM and/or CEO will respond to and comply with any information and enforcement notices served by the Commissioner or authorised officer.'	August 2024

Glossary of terms used in Data Protection Policy

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 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. The UK GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.

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 performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.[1]

Credit Union Personnel: all employees, workers, contractors, agency workers, consultants, directors, officer and volunteers.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Data relating to them.

Data Controller: the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the UK GDPR. We are the Data Controller of all Personal Data relating to our Credit Union Personnel and Personal Data used in our business for our own commercial purposes.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programs involving the Processing of Personal Data.

Data Protection Officer (DPO): the person required to be appointed in specific circumstances under the UK GDPR. ***The Board of Directors of Ballymena Credit Union have taken the decision not to appoint a mandatory DPO at this time. Where this term is used it refers to the data protection representative.***

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

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. It includes Special Category Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour. The personal data processed by the credit union has been identified in its Personal Data Register which is available on request from

[1] In a credit union context, this is most likely incurred (where the credit union utilises IT solutions) in the assessment of members to ensure compliance with anti-money laundering obligations

the DPO.

Personal Data Breach: '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'.

Personal Data Register: The document recording amongst other things, the personal data processed by the Credit Union including the legal ground being relied on for each Processing activity.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the UK GDPR.

Privacy Notices: separate notices setting out information that may be provided to Data Subjects when the Credit Union collects information about them. These notices may take the form of general privacy notices applicable to a specific group of individuals (for example, membership application forms, employee privacy notices or the website privacy policy or they may be stand-alone, one time privacy statements covering Processing related to a specific purpose (for example loan applications).

Processing or Process: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

Pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Related Policies: the Credit Union's policies, operating procedures or processes related to this policy and designed to protect Personal Data, as set out in Appendix 1 to this policy.

Special Category Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data

UK General Data Protection Regulation (UK GDPR): The UK GDPR is the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) (EU GDPR) as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 and as amended by Schedule 1 to the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (SI 2019/419).

1. Introduction

Ballymena Credit Union Limited, trading as Ballymena Causeway Credit Union and hereinafter referred to as "the Credit Union", holds personal data about its members, Credit Union Personnel, service providers, suppliers and other individuals for a variety of credit union purposes. The personal data held by the credit union includes the following:

> *Credit union account number, details of the credit union products you hold, Address data, bank data, contract data, signatures, identification documents, date of birth, email, telephone, salary, occupation, financial information, accommodation status, mortgage details, previous addresses, spouses, partners, nominations, National Insurance numbers, contact and address details, passport details, date of birth, interactions with credit union staff on the premises, by phone or email, current or past complaints, educational background, financial and pay details, details of certificates and diplomas, education and skills, nationality, job title, and CV, special category data such as declaration of health forms*

This information is necessary to allow the credit union to carry out its day to day operations, to meet its objectives and to comply with legal and regulatory obligations. Credit Union purposes include (but may not be limited to) the following:

- compliance with our legal, regulatory and corporate governance obligations and good practice;
- gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests;
- ensuring business policies are adhered to (such as policies covering email and internet use);
- operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of commercially sensitive information, security vetting,
- money laundering checks, fraud prevention, debt tracing and credit scoring;
- investigating complaints;
- checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments;
- monitoring staff conduct, disciplinary matters;
- marketing our credit union; and
- any other service(s) offered by the credit union to its members.

This policy sets out how the credit union seeks to protect personal data and ensure Credit Union Personnel understand the rules governing their use of personal data to which they have access in the course of their relationship with the credit union. This policy requires Credit Union Personnel to ensure that the **DPO should be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.** The credit union is committed to ensuring any personal data will be dealt with in line with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 1998.

This policy (together with Related Policies set out in Appendix 1) is an internal document and cannot be shared with third parties, clients, supervisory authorities[2] or regulators without prior authorisation from the Board of Directors.

[2] The Information Commissioner's Office (ICO)

The credit union recognises that Special Category Data merits higher protection.

2. Scope

This policy applies to all Credit Union Personnel. All Credit Union Personnel must be familiar with this policy and comply with its terms.

This policy supplements ~~our~~ other policies relating to data protection. The credit union may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to officers and volunteers before being adopted.

We recognise that the correct and lawful treatment of Personal Data will maintain confidence in not only this credit union but the wider credit union movement and will provide for successful business operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we always take seriously. The Credit Union is exposed to potential fines of up to EUR20 million or 4% of total worldwide annual turnover, whichever is higher and depending on the breach, for failure to comply with the provisions of the UK GDPR.

All parties are responsible for ensuring all Credit Union Personnel comply with this policy and need to implement appropriate practices, processes, controls and training to ensure such compliance.

The Board of Directors of Ballymena Credit Union have taken the decision not to appoint a mandatory DPO at this time. This decision is based on the premise that the credit union does not meet the criteria set out by the General Data Protection Regulations[3]. Instead, a decision has been taken to appoint a Data Protection Representative and Deputy Data Protection Representative. These individuals are responsible for overseeing this policy and, as applicable, developing Related Policies and privacy guidelines.

- **Data Protection Representative: Risk and Compliance Manager**
- **Deputy Data Protection Representative: Head of Operations**
- **Contact: info@ballymenacu.co.uk**

Please contact the above individuals with any questions about the operation of this policy or the UK GDPR or if you have any concerns that this policy is not being or has not been followed. Credit Union Personnel must always contact the DPO in the following circumstances:

(a) if you are unsure of the lawful basis which you are relying on to process Personal Data;
(b) if you need to rely on Consent and/or need to capture Explicit Consent;
(c) if you need to draft Privacy Notices;
(d) if you are unsure how long to keep the personal data being processed;
(e) if unsure about what security/other measures you need to use to protect Personal Data;
(f) if there has been a Personal Data Breach;
(g) if you are unsure on what basis to transfer Personal Data outside the EEA;

[3] Under the UK GDPR, you must appoint a DPO if:

• you are a public authority or body (except for courts acting in their judicial capacity);

• your core activities require large scale, regular and systematic monitoring of individuals (for example, online behaviour tracking); or

• your core activities consist of large-scale processing of special categories of data or data relating to criminal convictions and offences.

(h) if you need any assistance dealing with any rights invoked by a Data Subject;
(i) if you are engaging in a significant new, or change in, Processing activity which is likely to require a DPIA? or plan to use Personal Data for purposes other than it was collected for;
(j) If you plan to undertake any Automated Processing including profiling or Automated Decision-Making
(k) If you need help complying with applicable law when carrying out direct marketing activities; or
(l) if you need help with any contracts or other areas in relation to sharing Personal Data with third parties.

3. Who is responsible for this policy?

The Board of Directors have overall responsibility for this policy. They are responsible for ensuring this policy is adhered to by all Credit Union Personnel. Everyone within the credit union must observe this policy. The Board of Directors will have monitoring procedures in place to ensure it is being adhered to.

Credit Union Personnel will regularly review all the systems and processes under their control to ensure they comply with this policy and check that adequate governance controls and resources are in place to ensure proper use, Processing and protection of Personal Data.

4. Personal Data Protection Principles

The Credit Union is responsible for and must be able to demonstrate compliance with the data protection principles listed below:

The Credit Union adheres to the principles relating to Processing of Personal Data set out in the UK GDPR which require Personal Data to be:

Lawful, Fair and Transparent	Processed lawfully, fairly and in a transparent manner	**See section 5**
Purpose Limitation	Collected only for specified, explicit and legitimate purposes	**See section 7**
Data Minimisation	Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed	**See section 8**
Accurate	Accurate and where necessary kept up to date	**See section 9**
Storage Limitation	Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed	**See section 10**
Security, Integrity and Confidentiality	Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage	**See section 11**

Transfer Limitation	Not transferred to another country without appropriate safeguards being in place	**See section 13**
Data Subject's Rights and Requests	Made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data	**See section 14**

5. Lawfulness, Fairness and Transparency

5.1 Lawfulness and Fairness

Personal data must be Processed lawfully, fairly and in a transparent manner in relation to the Data Subjects.

The Credit Union only collects, Processes and shares Personal Data fairly and lawfully and for specified purposes, such purposes as are outlined in the credit union's Privacy Notices (see copy in Appendix 2). The UK GDPR restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent Processing, but ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.

The UK GDPR allows Processing where you have a legal basis for doing so, some of which are set out below;

(a) the Data Subject has given his or her **Consent**;
(b) the Processing is necessary for the **performance of a contract** with the Data Subject;
(c) to meet our **legal compliance obligations**;
(d) to protect the Data Subject's **vital interests**;
(e) to pursue our **legitimate interests** for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The purposes for which we process Personal Data for legitimate interests need to be set out in applicable Privacy Notices or Fair Processing Notices; or

The Credit Union will identify and document the legal ground being relied on for each Processing activity. This information is held in our Personal Data Register and is displayed on our Privacy Notices.

5. Consent

The Credit Union will only process Personal Data on the basis of one or more of the lawful bases set out in the UK GDPR, which include Consent.

A Data Subject consents to Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity will be insufficient. If Consent is given in a document which deals with other matters, then the Consent will be kept separate from those other matters. In this credit union, this will apply to the following areas:

- Direct Marketing consents
- Schools Quiz/Art Competition

Where the legal basis for the processing is identified by the credit union as 'consent' we will discontinue processing following withdrawal of that consent by the data subject. Consent may need to be refreshed if we intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

Unless we can rely on another legal basis of Processing, Explicit Consent is usually required for Processing Special Category Data, for Automated Decision-Making and for cross border data transfers. Usually we will be relying on another legal basis (and not require Explicit Consent) to Process most types of Special Category Data. Where Explicit Consent is required, you must issue a Fair Processing Notice to the Data Subject to capture Explicit Consent.

As well as having a legal basis for Processing Special Category Data, the Credit Union will have an appropriate pre-condition to process special category data. The Credit Union ensures this is documented.

We need to evidence when Consent is captured and keep records of all Consents so that the credit union can demonstrate compliance with Consent requirements. This evidence is kept in the following location(s):

- Member file on Progress System;
- Hard copy member file (Marketing Preference form)
- Secure files held by the Marketing Team.

6. Transparency (Notifying Data Subjects)

The UK GDPR requires Data Controllers to provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. Such information will be provided through appropriate Privacy Notices which will be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

Whenever we collect Personal Data directly from Data Subjects (including employment purposes), we must provide the Data Subject (which includes Credit Union Personnel, candidates for recruitment and nominees under nominations) with all the information required by the UK GDPR including the identity of the Data Controller and DPO, how and why we will use, Process, disclose, protect and retain that Personal Data through a Privacy Notice which must be presented when the Data Subject first provides the Personal Data. In most cases, this will be when a member applies to join the Credit Union or takes out a loan. Our separate privacy notices are set out and available at **Appendix 2.**

When Personal Data is collected indirectly (for example, from a third party or publicly available source), the Credit Union must provide the Data Subject with all the information required by the UK GDPR as soon as possible after collecting/receiving the data. The Credit Union must also check that the Personal Data was collected by the third party in accordance with the UK GDPR and on a basis which contemplates our proposed Processing of that Personal Data. Members will be asked to confirm that they have received a copy of the Privacy Notice(s) using a tick box format.

Privacy Notice(s) will be made available on the website (www.bccu.co.uk) and will be available in our offices in William Street Ballymena, Abbey Street Coleraine~~,~~

7. Purpose Limitation

Personal Data is only collected for specified, explicit and legitimate purposes. Personal data is not further Processed in any manner incompatible with those purposes. These purposes are records in our Personal Data Register.

The Credit Union will not use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless we have informed the Data Subject of the new purposes and they have Consented where necessary.

8. Data Minimisation

Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed. Credit Union Personnel will only Process Personal Data when performing their duties requires it. Credit Union Personnel cannot Process Personal Data for any reason unrelated to their duties.

Credit Union Personnel will only collect Personal Data that is required for their duties and must not collect excessive data. Credit Union Personnel should ensure that any Personal Data collected by them is adequate and relevant for the intended purposes.

Credit Union Personnel must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised safely and securely in accordance with the Credit Union's Data Retention Policy.

Credit Union Personnel ensure that they do not disclose personal data where there is no lawful basis for doing so. This includes taking steps to redact personal data from communications where that personal data is not necessary for the purpose of the communication.

9. Accuracy

Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

The Credit Union will ensure that the Personal Data we use, and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. Credit Union Personnel must check the accuracy of any Personal Data at the point of collection. Credit Union Personnel must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

10. Storage Limitation

Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed. The Credit Union must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

The Credit Union maintains a Retention Policy defining retention times where possible and these times take into consideration business needs and legal obligations to retain data. Our Retention Policy details procedures to ensure Personal Data is deleted after a reasonable time for the purposes for which it was being held.

The Credit Union will take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with our Retention Policy. This includes requiring third parties to delete such data where applicable.

The Credit Union will ensure Data Subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice(s). The retention period is also included in the Personal Data Register.

11. Security Integrity and Confidentiality

12. Protecting Personal Data

Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

The Credit Union will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data that we own or maintain on behalf of others and identified risks (including use of encryption/ Pseudonymisation/Anonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data.

The Credit Union is responsible for protecting the Personal Data we hold. The Credit Union implements reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data. The Credit Union will exercise particular care in protecting Special Category Data from loss and unauthorised access, use or disclosure.

Credit Union Personnel must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. The Credit Union will only transfer Personal Data

to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

The Credit Union will maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

- **Confidentiality** means that only people who have a need to know and are authorised to use the Personal Data can access it.
- **Integrity** means that Personal Data is accurate and suitable for the purpose for which it is processed.
- **Availability** means that authorised users can access the Personal Data when they need it for authorised purposes.

Credit Union Personnel must comply with all applicable aspects of the Credit Union's Information Security Policy.

13. Reporting a Personal Data Breach

The UK GDPR requires Data Controllers to notify any Personal Data Breach to the Information Commissioner's Office (ICO) and, in certain instances, the Data Subject.

The Credit Union has put in place procedures and a Data Breach Policy to deal with any suspected Personal Data Breach and will notify Data Subject, supervisory authority or any applicable regulator where we are legally required to do so.

If Credit Union Personnel know or suspect that a Personal Data Breach has occurred, they must not attempt to investigate the matter. **Credit Union Personnel must immediately consult the Data Breach Policy, contact the DPO (or in her absence the Deputy DPO) and follow the Credit Union's Data Breach Response Plan. All evidence relating to the potential Personal Data Breach must be preserved.**

RCM and/or CEO will respond to and comply with any information and enforcement notices served by the Commissioner or authorised officer.

14. Transfer Limitation

The UK GDPR restricts data transfers to countries outside the UK in order to ensure that the level of data protection afforded to individuals by the UK GDPR is not undermined. Personal Data is transferred when it originates in one country and it is transmitted, sent, viewed or accessed in or to a different country.

The Credit Union may only transfer Personal Data outside the UK if one of the following conditions applies:

- the UK Government has issued a decision confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subjects' rights and freedoms;
- appropriate safeguards are in place such as binding corporate rules (BCR), standard contractual clauses approved by the UK Government, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the DPO;
- the Data Subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks; or
- the transfer is necessary for one of the other reasons set out in the UK GDPR including the performance of a contract between us and the Data Subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent and, in some limited cases, for our legitimate interest.

15. Data Subject's Rights and Requests

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

a	**withdraw** Processing based on Consent at any time;
b	**receive** certain information about the Data Controller's Processing activities;
c	**request** access to their Personal Data that we hold;
d	**prevent** our use of their Personal Data for direct marketing purposes;
e	**ask us to erase** Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;
f	**restrict** Processing in specific circumstances;
g	**challenge** Processing which has been justified on the basis of our legitimate interests or in the public interest;
i	**object** to decisions based solely on Automated Processing, including profiling (ADM)[4];
k	be **notified** of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;
l	**make a complaint** to the supervisory authority; and
m	**in limited circumstances, receive or ask** for their Personal Data to be transferred to a third party in a structured, commonly used and machine-readable format[5].

Credit Union Personnel will verify the identity of an individual requesting data under any of the rights listed above (They should not allow third parties to persuade them into disclosing Personal Data without proper authorisation).

Credit Union Personnel must immediately forward any Data Subject request received to the DPO or in her absence to the Deputy DPO.

16. Accountability

The Credit Union will implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. The Credit Union is responsible for, and must be able to demonstrate, compliance with the data protection principles.

The Credit Union will ensure that adequate resources and controls are in place to comply with and document GDPR compliance including:

- appointing a suitably qualified DPO (where necessary) and where appropriate identifying a director with specific responsible for liaison between the DPO and board. **The Credit Union has appointed a Data Protection Representative and a Deputy Data Protection Representative.**
- implementing Privacy by Design when Processing Personal Data and completing DPIAs where Processing presents a high risk to rights and freedoms of Data Subjects;
- integrating data protection into internal documents including this policy, Related Policies, privacy guidelines, Privacy/Fair Processing Notices;
- regularly training Credit Union Personnel on the UK GDPR, this policy, Related Policies and privacy guidelines and data protection matters; and

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

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

- regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

17. Training

All Credit Union Personnel will receive training on this policy. New joiners will receive training as part of their induction process. Further training will be provided at least annually or whenever there is a substantial change in the law or the Credit Union's policy and procedures.

Training is provided online via CU Learn or via weekly in-house training sessions. It will cover:

- the law relating to data protection; and
- our data protection and related policies and procedures

Completion of training is compulsory.

The Senior Management Team will continually monitor training needs but if Credit Union Personnel feel that further training on any aspect of the relevant law or our data protection policy or procedures is required, please contact your line manager directly.

18. Privacy by Design and Data Protection Impact Assessment (DPIA)

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

Credit Union Personnel will assess what Privacy by Design measures can be implemented on all programs/systems/processes that Process Personal Data by considering the following:

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

The Credit Union will also conduct DPIAs in respect any Processing which is high risk.

Credit Union Personnel must conduct a DPIA (and discuss any findings with the DPO) when implementing major system or business change programs involving the Processing of Personal Data including:

- use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);
- Automated Processing including profiling and ADM;
- large scale Processing of Special Category Data (such as health); and
- large scale, systematic monitoring of a publicly accessible area.

A DPIA will include:

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

19. Direct Marketing

The Credit Union is subject to certain rules and privacy laws when marketing to our members and non-members. The credit union has identified consent as the legal basis upon which it will conduct direct marketing.

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

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

A Data Subject's objection to direct marketing must be promptly honoured. If a customer opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

Credit Union Personnel must comply with the Credit Union's Marketing Policy.

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

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

The Credit Union will only share the Personal Data we hold with third parties, such as our service providers if:

- they have a need to know the information for the purposes of providing the contracted services;
- sharing the Personal Data complies with the Privacy/Fair Processing Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;
- the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
- the transfer complies with any applicable cross border transfer restrictions; and
- a fully executed written contract that contains UK GDPR approved third party clauses has been obtained.

20. Automated Processing (including Profiling) and Automated Decision Making (ADM)

Generally, ADM is prohibited when a decision has a legal or similar significant effect on an individual unless:

i. a Data Subject has Explicitly Consented;

ii. the Processing is authorised by law; or

iii. the Processing is necessary for the performance of or entering into a contract.

If certain types of Special Category Data are being processed, then grounds (b) or (c) will not be allowed but such Special Category Data can be Processed where it is necessary (unless less intrusive means can be used) for substantial public interest like fraud prevention.

If a decision is to be based solely on Automated Processing (including profiling), then Data Subjects will be informed when we first communicate with them of their right to object. This right will be explicitly brought to their attention

and presented clearly and separately from other information. Further, suitable measures will be put in place to safeguard the Data Subject's rights and freedoms and legitimate interests.

We will also inform the Data Subject in our privacy notice of the logic involved in the decision making or profiling, the significance and envisaged consequences and give the Data Subject the right to request human intervention, express their point of view or challenge the decision.

A DPIA will be carried out before any Automated Processing (including profiling) or ADM activities are undertaken.

21. Consequences of failing to comply

The board of directors take compliance with this policy very seriously. Failure to comply puts Credit Union Personnel and the Credit Union at risk.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under the credit union's procedures, which may result in dismissal.

22. Policy Review

This policy is formally reviewed on an annual basis or whenever there is a change in circumstance of the credit union.

Appendix 1

List of Related Policies/Documents

- **Data Breach Policy including response plan**
- **Office Security Policy**
- **Records Management and Retention Policy**
- **Privacy Notice(s)**
- **Information Security Policy**
- **CCTV Policy**

Appendix 2

Privacy Notices

- **Privacy Notice for Account Opening (Adult Accounts)**
- **Privacy Notice for Account Opening (Minor Accounts)**
- **Privacy Notice for Credit Union Personnel**
- **Privacy Notice for Nominations**
- **Privacy Notice for Recruitment**
- **Privacy Notice for Lending**
- **Privacy Notice for Guarantors**