



ROSENORT
CREDIT UNION LIMITED

Code for the Protection of Personal Information

TABLE OF CONTENTS

1.0 DEFINITIONS

2.0 INTRODUCTION

- 1.1 Purpose & Scope
- 1.2 Roles and Responsibilities - Privacy Officer
- 1.3 Roles and Responsibilities - Employees

3.0 PRIVACY POLICY

- 3.1 Policy Statement – Commitment to Members
- 3.2 Appoint Privacy Officer
- 3.3 Phased in Compliance
- 3.4 Staff Training
- 3.5 Annual Review

4.0 ¹ CODE FOR THE PROTECTION OF PERSONAL INFORMATION

- 4.1 Accountability
- 4.2 Identifying Purposes:
- 4.3 Consent
- 4.4 Limiting Collection
- 4.5 Limiting Use, Disclosure, and Retention
- 4.6 Accuracy
- 4.7 Safeguards
- 4.8 Openness
- 4.9 Individual Access
- 4.10 Compliance ²

FORWARD

Rosenort Credit Union Limited is committed to keeping members' personal information accurate, confidential, secure and private. This document sets forth the protective measures necessary to fully incorporate privacy practices into all information handling activities, and to foster the necessary levels of employee awareness and engagement.

This privacy code applies throughout Rosenort Credit Union Limited .

1.0 DEFINITIONS

The following definitions apply in this Code.

“Collection”

The act of gathering, acquiring, or obtaining personal information from any source, including Third Parties, by any means.

“Consent”

Voluntary agreement with what is being done or proposed. Consent can be either express or implied. Express consent is given explicitly, either orally or in writing. Express consent is unequivocal and does not require any inference on the part of the credit union or the Credit Union seeking consent. Implied consent arises where consent may reasonably be inferred from the action or inaction of the member.

“Privacy Officer” [Designated Individual]

The person within the Credit Union who is responsible for collection, use, disclosure and protection of members' personal information and the Credit Union's day-to-day compliance with the Code.

“Disclosure”

Making personal information available to others outside the Credit Union.

“Member” [Individual]

The person who is a member and owner of the credit union. This code applies equally to the collection, use or disclosures of personal information about members and non-members. Where the term “member” is used, its intent is also to include non-members.

“Organization”

A term used in the Code that includes organizations, partnerships, associations, businesses, charitable organizations, clubs, government bodies, institutions, professional practices and unions.

“Personal information”

Any information that is about or can be linked to an identifiable individual. This does not include the name, title or business address or business telephone number of an employee of an organization.

“Subsidiary”

A company or organization wholly-owned or controlled by a credit union, CUCM, CUCC, or other members of the Canadian financial co-operative sector.

“Third Party”

Any person or organization other than a credit union, CUCM, or member.

“Use”

Refers to the treatment and handling of personal information within the credit union or CUCM.

2.0 INTRODUCTION

2.1 Purpose & Scope

This document defines Rosenort Credit Union Limited (the Credit Union)'s Privacy Code, which provides guidelines that the Credit Union uses to protect the privacy of personally identifiable member and employee data that is collected, used, disclosed or communicated to the Credit Union by other financial institutions. This Code is based on the 10 privacy protection principles laid out in the Canadian Standards Association (CSA) *Model Code for the Protection of Personal Information* and applies to all aspects of information handling within the Credit Union.

2.2 Roles and Responsibilities – Privacy Officer

The prime responsibility for compliance with all of the principles of the Credit Union's Privacy Code resides with the Credit Union's Privacy Officer. However, this does not, in any way, relieve any other Credit Union employee from an obligation to comply with the law.

2.3 Roles and Responsibilities - Employees

All employees are responsible for maintaining the confidentiality of all personal information to which they have access. All employees are required to sign a "Oath of Office" agreement as a condition of employment, which, among other practices, confirms employee's commitment to safeguarding of all confidential information. This confirmation is reaffirmed annually.

3.0 PRIVACY POLICY

Rosenort Credit Union Limited's Privacy Policy is based on the CSA Privacy Code and informs the public of our commitment to individual privacy.

3.1 Policy Statement

The Board of Directors and the Management of the Credit Union are committed to ensuring the application of this policy in relation to the collection, usage, disclosure, and processing of personal data.

3.2 Appoint Privacy Officer

The Credit Union will designate a Privacy Officer who is accountable for the Credit Union's compliance with the principles of this Code. The Credit Union shall identify internally and to the system, the designated individual who is responsible for the organization's day-to-day compliance with the principles.

3.3 Phased in Compliance

The Credit Union will follow a phased in implementation of the Privacy Legislation.

3.4 Staff Training

The Privacy Officer will develop information and training materials to ensure employees clearly understand their obligations to protect personal information and the procedures to be employed under the the Credit Union Privacy Code.

3.5 Annual Review of Privacy Code

The Privacy Officer will review the Privacy Code on an annual basis and provide any recommendations or changes to senior management and the Board of Directors. The Privacy Officer also will report to the Board on the disposition of all inquiries to the Credit Union from their members, the public, other organizations, and government agencies.

4.0 CODE FOR THE PROTECTION OF PERSONAL INFORMATION

Ten interrelated principles form the basis of the Credit Union's Code for the Protection of Personal Information ("the Code").

4.1. Accountability

The Credit Union is responsible for personal information under its control and shall designate an individual who is accountable for the Credit Union's compliance with the principles of the Code.

Ultimate accountability for the Credit Union's compliance with the principles rests with the Credit Union's Board of Directors. Other individuals within the Credit Union may be accountable for the day-to-day collection and processing of personal information, or to act on behalf of a designated individual.

The Credit Union shall identify internally and to its members the designated individual who is responsible for the day-to-day compliance with the principles.

The Credit Union is responsible for personal information in its possession. The Credit Union shall use contractual or other means to provide a comparable level of protection while the information is being transmitted to or processed by a Third Party.

The Credit Union shall implement policies and procedures to give effect to the principles, including:

- procedures to protect personal information;
- procedures to receive and respond to concerns and inquiries;
- training staff to understand and follow the Credit Union's policies and procedures;
- annual review of the effectiveness of the policies and procedures to ensure compliance with the Code and consideration of revisions as deemed appropriate.

4.2 Identifying Purposes

The purposes for which personal information is collected shall be identified by the Credit Union at or before the time the information is collected.

The Credit Union shall document the purposes for which personal information is collected prior to the information being collected.

The Credit Union shall make reasonable efforts to ensure that individuals are aware of the purposes for which their personal information is collected, including use by Third Parties.

The Credit Union shall collect personal information for the following purposes:

- to meet legal and regulatory requirements
- to provide ongoing service
- to set up, offer, and manage products and services that meet member needs
- to aid in understanding member needs
- to assess conflicts of interest
- to perform internal and external audits
- to provide Corporate Governance Reports

- to provide credit checks on new employees
- to provide credit checks for employee mortgages

The identified purposes should be specified to the individual from whom the personal information is being collected. This can be done orally, electronically, or in writing. An application form with the purposes clearly identified, for example, may give notice of the purposes.

When personal information that has been collected is to be used for a purpose not previously identified, the new purpose shall be identified prior to use. Unless the new purpose is required by law, the consent of the individual is required before the information can be used for that purpose.

4.3 Consent

With few exceptions, the acknowledgment and consent of the individual is required for the collection, use, or disclosure of their personal information.

Note: In certain circumstances personal information may be collected, used, or disclosed without the knowledge and consent of the individual. These circumstances include:

- where disclosure is clearly in the interests of the individual and consent cannot be obtained in a timely way;
- to avoid compromising information availability or accuracy and, if reasonable, to investigate a breach of an agreement or a contravention of the laws of Canada or a province;
- where the information is generally considered to be in the public domain;
- to act in respect of an emergency that threatens the life, health, or security of an individual;
- assist in the investigation of an offense under the laws of Canada, a threat to Canada's security, to comply with a subpoena, warrant or court order or rules of a court relating to the production of records, or otherwise as required by law.

Consent is required for the collection of personal information and the subsequent use or disclosure of this information. In certain circumstances, consent may be sought after the information has been collected but before use (for example, when the Credit Union wants to use information for a purpose not previously identified). The Credit Union may be required to collect, use, or disclose personal information without the individual's consent for certain purposes, including the collection of overdue accounts, legal, or security reasons.

The principle requires "knowledge and consent". The Credit Union shall make reasonable effort to ensure that the Individual is aware of the purposes for which their information will be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how their information will be used or disclosed.

The Credit Union shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfill explicitly specified and legitimate purposes.

In determining the form of consent to use, the Credit Union shall take into account the sensitivity of the

information. Although some information (for example, medical and income records) is almost always considered to be sensitive, any information can be sensitive, depending on the context. When in doubt, employees should consult the Credit Union Privacy Officer before taking action that could jeopardize an individual's privacy.

The Credit Union will not obtain consent to carry out processing functions, such as data processing, secondary support, testing new products, cheque processing, etc. On the other hand, an individual would not reasonably expect that personal information given to the Credit Union would be given to a Third Party company selling insurance products, unless consent was obtained. Consent will not be obtained through deception.

The way in which the Credit Union seeks consent may vary, depending on the circumstances and the type of information collected. The Credit Union will seek express consent when the information is likely to be considered sensitive. Implied consent would generally be appropriate when the information is less sensitive.

Individuals can give consent:

- in writing, such as when completing and signing an application or applying for employment;
- through inaction, such as failing to check a box indicating that they do not wish their names and addresses to be given to other organizations;
- orally, such as when information is collected over the telephone or in person;
- at the time they use a product or service
- through an authorized representative (such as a legal guardian or a person having power of attorney).

An individual may withdraw consent at any time, subject to legal or contractual restrictions, provided that:

- reasonable notice of withdrawal of consent is given to the Credit Union;
- consent does not relate to a credit product requiring the collection and reporting of information after credit has been granted; and
- the withdrawal of consent is in writing and includes understanding by the individual that withdrawal of consent could mean that the Credit Union cannot provide the individual with a related product, service or information of value. The Credit Union shall inform the individual of the implication of such withdrawal.

4.4 Limiting Collection

The collection of personal information shall be limited to that which is necessary for the purposes identified by the Credit Union. Information shall be collected by fair and lawful means.

The Credit Union shall not collect personal information indiscriminately. The Credit Union shall specify both the amount and the type of information collected, limited to that which is necessary to fulfill the purposes identified, in accordance with the Credit Union's policies and procedures.

The Credit Union shall collect personal information by fair and lawful means, and not be misleading or deceiving individuals about the purpose for which information is being collected.

4.5 Limiting Use, Disclosure, and Retention

Personal information shall not be used or disclosed for purposes other than those for which it was

collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.

When the Credit Union uses personal information for a new purpose, the purpose shall be documented and will be provided to the Privacy Officer as required.

The Credit Union may disclose personal information without consent to protect the interests of the Credit Union or when required by law, for example, when requested:

- by subpoena or search warrant;
- by other court and government orders;
- by demands from other parties who have a legal right to personal information;
- by a person acting in a confidential or professional relationship with the Credit Union, such as an auditor or a solicitor.

The Credit Union shall protect the interests of credit union members and the Credit Union employees by taking reasonable steps to ensure that:

- orders or demands comply with the laws under which they were issued;
- only the personal information that is legally required is disclosed and nothing more;
- casual requests for personal information are denied;
- personal information disclosed to unrelated Third Party suppliers of non-financial services is strictly limited to programs endorsed by the Credit Union.

The individual's health records at the Credit Union may be used for credit application and related insurance purposes or as required for the provision of individual health insurance or benefits. The individual's health records shall not be collected from, or disclosed to, any other organization.

The Credit Union shall maintain guidelines and procedures with respect to the retention of personal information. These guidelines include minimum and maximum retention periods. Personal information that has been used to make a decision about an individual shall be retained long enough to allow the individual access to the information after the decision has been made. The Credit Union may be subject to legislative requirements with respect to retention of records.

Subject to any requirement to retain records, personal information that is no longer required to fulfill the identified purposes shall be destroyed, erased, or made anonymous. the Credit Union shall develop guidelines and implement procedures to govern the destruction of personal information.

4.6 Accuracy

Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

The extent to which personal information shall be accurate, complete, and up-to-date will depend upon the use of the information, taking into account the interests of the individual. The Credit Union relies on the individual to keep certain personal information accurate, complete and current, such as name and address. Information shall be sufficiently accurate, complete, and up-to-date to minimize the possibility

that inappropriate information may be used to make a decision about the individual.

The Credit Union shall not routinely update personal information, unless such a process is necessary to fulfill the purposes for which the information was collected.

Personal information that is used on an on-going basis, including information that is disclosed to Third Parties, will generally be accurate and up-to-date unless limits to the requirement for accuracy are clearly set out.

4.7 Safeguards

Security safeguards appropriate to the sensitivity of the information shall protect personal information. The Credit Union will employ the same standard of care as it takes to safeguard its own confidential information of a similar nature.

The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. The Credit Union shall protect personal information regardless of the format in which it is held.

The nature of the safeguards will vary depending on the sensitivity, amount, distribution and format of the information, and the method of storage. A higher level of protection will safeguard more sensitive information.

The methods of protection will include:

- physical measure, for example, locked filing cabinets and restricted access to offices;
- organizational measures, for example, controlling entry to data centers and limiting access to information to a "need-to-know" basis;
- technological measures, for example, the use of passwords and encryption;
- investigative measures, in cases where the Credit Union has reasonable grounds to believe that personal information is being inappropriately collected, used or disclosed.

The Credit Union shall periodically remind employees, Directors, and Officers of the importance of maintaining the confidentiality of personal information. Employees and Directors are individually required to sign the "Oath of Office" annually, including commitment to keep member's personal information in strict confidence.

Third Parties shall be required to safeguard personal information disclosed to them in a manner consistent with the policies of the Credit Union. Examples include cheque processing, credit collection, credit bureau, and card production.

Care shall be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information.

4.8 Openness

The Credit Union shall make readily available specific, understandable information about its policies and

practices relating to the management of personal information.

The Credit Union shall be open about privacy policies and procedures with respect to the management of personal information and shall make them readily available in a form that is generally understandable.

The information made available shall include:

- the name or title and the address of the designated individual who is accountable for compliance with the Credit Union policies and procedures and to whom complaints or inquiries can be forwarded;
- the means of gaining access to personal information held by the Credit Union;
- a description of the type of personal information held by the Credit Union, including a general account of its use;
- a copy of any brochures or other information that explains the Credit Union policies, procedures, standards or codes;
- the types of personal information made available to related organizations, such as subsidiaries or other suppliers.

The Credit Union may make information on its policies and practices available in a variety of ways. The method chosen depends on the nature of its business and other considerations. For example, the Credit Union may choose to make brochures available in its place of business, by mail, through on-line access, or through a toll-free telephone number.

4.9 Individual Access

Upon request, an individual shall be informed of the existence, use, and disclosure of their personal information, and shall be given access to that information. An individual is entitled to challenge the accuracy and completeness of the information and have it amended as appropriate.

Note: In certain situations, the Credit Union may not be able to provide access to all the personal information it holds about an individual. Exceptions to the access requirement will be limited and specific. The reasons for denying access include the following:

- providing access would likely reveal personal information about a third party (unless such information can be severed from the record or the third party consents to the disclosure, or the information is needed due to a threat to life, health or security);
- the personal information has been requested by a government agency to enforce any law of Canada, a province or a foreign jurisdiction, to carry out any investigation related to the enforcement of any law, the administration of any law, the protection of national security, the defense of Canada or the conduct of international affairs;
- the information is protected by solicitor-client privilege;
- providing access would reveal confidential commercial information, (provided this information cannot be severed from the file containing other information requested by the individual);
- providing access could reasonably be expected to threaten the life or security of another individual, (provided this information cannot be severed from the file containing other information requested by the individual);
- the information was collected without the knowledge or consent of the individual for purposes related to

investigating a breach of an agreement or a contravention of the laws of Canada or a province;
- the information was generated in the course of a formal dispute resolution process.

Upon request, the Credit Union shall inform an individual of the existence, use, disclosure, and source of personal information about the individual held by the Credit Union, and shall allow the individual access to this information. However, the Credit Union may choose to make sensitive medical information available through a medical practitioner rather than by communicating it directly to the individual.

For the Credit Union to provide an account of the existence, use, and disclosure of personal information held by the Credit Union, the individual may be asked to provide sufficient information to aid in the search. The additional information provided shall only be used for this purpose.

In providing an account of Third Parties to which it has, or may have, disclosed personal information about an individual the Credit Union will be as specific as possible, including a list of Third Parties.

The Credit Union shall respond to an individual's request within a reasonable time and at no cost, or at a reasonable cost, to the individual. The requested information shall be provided or made available in a form that is generally understandable. For example, if the Credit Union uses abbreviations or codes to record information, an explanation will be provided.

When an individual successfully demonstrates the inaccuracy or incompleteness of personal information, the Credit Union shall amend the information as required. Depending upon the nature of the information challenged, amendment involves the correction, deletion, or addition of information. Where appropriate, the amended information shall be transmitted to Third Parties having access to the information in question.

When a challenge is not resolved to the satisfaction of the individual, the substance of the unresolved challenge shall be recorded by the Credit Union. When appropriate, the existence of the unresolved challenge shall be transmitted to Third Parties having access to the information in question.

4.10 Compliance

An individual shall be able to question compliance with the above principles to the designated individual accountable for the Credit Union's compliance. The Credit Union shall have policies and procedures in place to respond to an individual's questions and concerns.

The name of and how to contact the Credit Union Privacy Officer shall be communicated to the Credit Union staff and the Manitoba credit union system.

The Credit Union shall maintain procedures to receive and respond to complaints or inquiries about their policies and practices relating to the handling of personal information. The complaint procedures will be easily accessible and simple to use.

Individuals who make inquiries or lodge complaints shall be informed by the Credit Union of the existence of relevant complaint procedures. If a complaint is not satisfactorily resolved by the Credit Union's Privacy

Officer, it may be taken to the Credit Union's Board of Directors. If not resolved there, procedures shall be in place to refer it to a regulator. The Credit Union shall inform individuals of their right to file a complaint with the Privacy Commissioner of Canada.

The Credit Union shall investigate all complaints. If a complaint is found to be justified, the Credit Union shall take appropriate measures, including revision of the personal information and, if necessary, amending the Credit Union's policies and practices.