
Code for the Protection of Personal Information



First Adopted by:
Prairie Centre Credit Union Board of Directors
July 15, 2003

Updated/Reviewed:
November 2014
October 2019
December 2022

Introduction

Prairie Centre Credit Union (PCCU) and its employees have always been committed to keeping our member personal information accurate, confidential, secure and private. The Privacy Code that follows builds on this commitment. This code is based on the Credit Union Central of Canada Model Privacy Code and on the Model Code for the Protection of Personal Information (CAN/CSA-Q830-96) included as Schedule 1 of the federal *Personal Information Protection and Electronic Documents Act (revised May 2019)*. This Code describes how Prairie Centre Credit Union subscribes to the principles set out in those model codes.

Principles

Principles form the basis of the Prairie Centre Credit Union Code for the protection of Personal Information ("the Code"). Each principle must be read in conjunction with the accompanying commentary.

1. Accountability

PCCU is responsible for personal information under its control and has designated a Privacy Officer who is accountable for the credit union's compliance with the principles of the Code.

2. Identifying Purposes

The purposes for which personal information is collected will be identified by PCCU at or before the information is collected.

3. Consent

The knowledge and consent of the member are required for the collection, use, or disclosure of personal information, except in specific circumstances as described within this Code.

4. Limiting Collection

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

5. Limiting Use, Disclosure, and Retention

Personal information will not be used or disclosed for purposes other than those for which it was collected, except with the consent of the member or as required by law. Personal information will be retained only as long as necessary for the fulfilment of those purposes.

6. Accuracy

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

7. Safeguards

Personal information will be protected by security safeguards appropriate to the sensitivity of the information. PCCU will apply the same standards of care as it applies to safeguard its own confidential information of a similar nature.

8. Openness

PCCU will make readily available to members specific, understandable information about its policies and practices relating to the management of personal information.

9. Individual Access

Upon request, a member will be informed of the existence, use, and disclosure of their personal information, and will be given access to that information. A member is entitled to challenge the accuracy and completeness of the information and have it amended as appropriate. In certain situations, PCCU may not be able to provide access to all the personal information it holds about a member. Exceptions to the access requirement will be limited and specific.

10. Challenging Compliance

A member will be able to question compliance with the above principles to PCCU's Privacy Officer. PCCU has policies and procedures in place to respond to member questions and concerns.

11. Breach Notification, Reporting & Record Keeping

PCCU will keep records of all privacy breaches. Where there is a real risk of significant harm PCCU notify individuals and report to the Privacy Commissioner.

Definitions

Business Contact Information

Any information used for the purpose of communicating with an individual in relation to their employment, business or profession such as name, position or title, work address, telephone or fax numbers, work electronic address.

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 PCCU. Implied consent arises where consent may reasonably be inferred from the action or inaction of the Member.

Disclosure

Making personal information available to others outside PCCU.

Member

Includes members and non-members that receive financial services from PCCU.

Organization

Includes an organization, partnership, association, business, charitable organization, club, government body, institution, professional practices and unions.

Person

Includes an individual and an entity.

Personal information

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

Privacy Breach

Any loss of unauthorized access to, or unauthorized disclosure of personal information, whether identified internally or externally.

Privacy Officer

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

Subsidiary

A company or organization wholly owned or controlled by PCCU.

Third Party

Any person or organization other than PCCU or the member.

Use

The treatment and handling of personal information within PCCU.

Principles

Principle 1 – Accountability

1.0 PCCU is responsible for personal information under its control and has designated a Privacy Officer who is accountable for PCCU's compliance with the principles of this Code.

1.1 Ultimate accountability for PCCU's compliance with the principles rests with the PCCU Board of Directors, who delegates day-to-day accountability to the Privacy Officer. Other individuals within PCCU may be accountable for the day-to-day collection and processing of personal information, or to act on behalf of the Privacy Officer.

1.2 PCCU will identify to its employees and to its members the Privacy Officer who is responsible for the day-to-day compliance with the principles.

1.3 PCCU is responsible for personal information in its control. PCCU will use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.

1.4 PCCU has implemented policies and procedures to give effect to the principles, including:

- a) procedures to protect personal information;
- b) procedures to receive and respond to concerns and inquiries;
- c) training staff to understand and follow PCCU's policies and procedures; and
- d) bi-ennial review of the effectiveness of the policies and procedures to ensure compliance with the Code and consideration of any revisions as deemed appropriate.

Principle 2 - Identifying Purposes

2.0 The purposes for which personal information is collected will be identified by PCCU when or before the information is collected.

2.1 PCCU will document the purposes for which personal information is collected prior to the information being collected.

2.2 PCCU will make reasonable efforts to ensure that members are aware of the purposes for which personal information is collected, including any disclosures to third parties.

2.3 Identifying the purposes for which personal information is being collected at or before the time of collection and defining the information needed to fulfill these purposes. PCCU will collect personal information for the following purposes:

- to understand the member's needs;
- to determine the suitability of the products or services for the member or the eligibility of the member for products and services;
- to develop, offer and manage products and services to meet the member's needs;
- to detect and prevent fraud, and to help safeguard the financial interests of PCCU and its members;
- to meet legal and regulatory requirements; and
- to meet personnel requirements.

2.4 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 highlighted, for example, may give notice of the purposes.

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

Principle 3 – Consent

3.0 Where clearly in the interests of individuals:

The knowledge and consent of the member is required for the collection, use, or disclosure of personal information, except in specific circumstances as described within this Code.

In certain circumstances personal information may be collected, used, or disclosed without the knowledge or consent of the member. These circumstances include, but are not limited to:

- the collection is clearly in the interests of the member 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 considered by law to be publicly available;

- to act in respect of an emergency that threatens the life, health or security of a member;
- to investigate an offence under the laws of Canada, a threat to Canada's security, to comply with a subpoena, warrant or court order, or rules of court relating to the production of records, or otherwise as required by law
- a government institution or next of kin if the individual has been or may be the victim of financial abuse, and disclosure is made for the purpose of preventing or investigating the abuse. It must be reasonable to expect the disclosure with knowledge and consent would compromise the ability to prevent or investigate the abuse.
- communicating with next of kin;
- identification of an injured, ill or deceased person.

NOTE: This is not an exhaustive list. You should always check with the Privacy Officer before disclosing personal information without consent and/or knowledge of the member.

3.1 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 existing information is to be used for a purpose not previously identified).

PCCU may be required to collect, use, or disclose personal information without a member's consent for certain purposes, including the collection of overdue accounts, legal or security reasons.

3.2 The principle requires "knowledge and consent". PCCU will make a reasonable effort to ensure that members are aware of the purposes for which the information will be used.

To make the consent meaningful, the purposes must be stated in such a manner that the member can reasonably understand how the information will be used or disclosed.

3.3 PCCU will not, as a condition of the supply of a product or service, require a member to consent to the collection, use, or disclosure of information beyond that required to fulfill explicitly specified and legitimate purposes.

3.4 In determining the form of consent to use, PCCU will take into account the sensitivity of the information. Although some information (for example, medical and financial records) is almost always considered to be sensitive, any information can be sensitive depending on the context.

3.5 In obtaining consent, the reasonable expectations of the member are relevant. For example, a member should reasonably expect PCCU to periodically supply information on credit union developments, products and services, and to provide ongoing services.

Similarly, further consent will not be required when personal information is transferred to agents of PCCU to carry out functions such as data processing. In this case, PCCU can assume that the member's request constitutes consent for specifically related purposes.

On the other hand, a member would not reasonably expect that personal information given to PCCU would be given to a third-party company selling insurance products, unless consent was obtained.

Consent will not be obtained through deception.

3.6 The way in which PCCU seeks consent may vary, depending on the circumstances and the type of information collected. PCCU 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. Members can give consent:

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

3.7 A member may withdraw consent at any time, subject to legal or contractual restrictions, provided that:

- a) reasonable notice of withdrawal of consent is given to PCCU;
- b) consent does not relate to a credit product requiring the collection and reporting of information after credit has been granted; and
- c) the withdrawal of consent is in writing and includes understanding by the member that withdrawal of consent could mean that PCCU cannot provide the member with a related product, service or information of value.
- d) PCCU will inform the member of the implications of such withdrawal.

Principle 4 – Limiting Collection

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

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

4.2 PCCU will collect personal information by fair and lawful means, and not by misleading or deceiving members about the purpose for which information is being collected.

Principle 5 – Limiting Use, Disclosure, and Retention

5.0 Personal information will not be used or disclosed for purposes other than those for which it was collected, except with the consent of the member or as required by law. Personal information will be retained only as long as necessary for the fulfillment of those purposes.

5.1 When PCCU uses personal information for a new purpose, the purpose will be documented.

5.2 PCCU will 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 a member will be retained long enough to allow the member access to the information after the decision has been made. PCCU may be subject to legislative requirements with respect to retention of records.

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

5.4 PCCU will protect the interests of its members by taking reasonable steps to ensure that:

- a) orders or demands comply with the laws under which they were issued;
- b) only the personal information that is legally required is disclosed and nothing more;
- c) casual requests for personal information are denied; and

- d) personal information disclosed to unrelated third parties of non-financial services is strictly limited to programs endorsed by PCCU.

PCCU will make reasonable efforts to notify the member that an order has been received, if not contrary to the security of PCCU and if the law allows it. Notification may be by telephone, or by letter to a member's usual address.

5.5 The member's health records at PCCU may be used for credit applications and related insurance purposes. These health records will not be collected from, or disclosed to, any other organization.

Principle 6 – Accuracy

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

6.1 The extent to which personal information will be accurate, complete, and up-to-date will depend upon the uses of the information, taking into account the interests of the member. PCCU relies on the member to keep certain personal information, accurate, complete and up-to-date.

Information will be sufficiently accurate, complete, and up-to-date to minimize the possibility that inappropriate information may be used to make a decision about a member.

6.2 PCCU will not routinely update personal information, unless such a process is necessary to fulfill the purposes for which the information was collected.

6.3 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.

Principle 7 – Safeguards

7.0 Personal information will be protected by security safeguards appropriate to the sensitivity of the information. PCCU will apply the same standard of care as it applies to safeguard its own confidential information of a similar nature.

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

7.2 The nature of the safeguards will vary depending on the sensitivity, amount, distribution and format of the information, and the method of storage. More sensitive information will be safeguarded by a higher level of protection.

7.3 The methods of protection will include:

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

7.4 PCCU will periodically remind employees, officers and directors of the importance of maintaining the confidentiality of personal information.

Each senior officer and director annually completes a declaration agreeing to the terms of the Code of Conduct. Upon successful completion of the annual online Code of Conduct exam, all other employees accept the terms and conditions of the declaration.

7.5 Care will be taken in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information.

7.6 Third parties will be required to safeguard personal information disclosed to them in a manner consistent with the policies of PCCU.

Examples include cheque printing, data processing, credit collection, credit bureaus and card production.

7.7 A record of every breach of security safeguards involving personal information will be kept and maintained.

Principle 8 – Openness

8.0 PCCU will make readily available specific, understandable information about its policies and procedures relating to the management of personal information.

8.1 PCCU will be open about privacy policies and procedures with respect to the management of personal information and will make them readily available in a format that is generally understandable.

8.2 The information made available will include:

- a) the name or title, and the address of the Privacy Officer who is accountable for compliance with PCCU's policies and procedures and to whom inquiries or complaints can be forwarded;
- b) the means of gaining access to personal information held by PCCU;
- c) a description of the type of personal information held by PCCU, including a general account of its use;
- d) a copy of any brochures or other information that explains PCCU's policies, procedures, standards or codes; and
- e) the types of personal information made available to related organizations such as subsidiaries or other suppliers of services.

8.3 PCCU may make information on its policies and procedures available in a variety of ways. The method chosen depends on the nature of its business and other considerations. For example, PCCU may choose to make brochures available in its place of business, mail information to members, provide on-line access, or establish a toll-free telephone number.

Principle 9 – Individual Access

9.0 Upon request, a member will be informed of the existence, use, and disclosure of their personal information, and will be given access to that information. A member is entitled to challenge the accuracy and completeness of the information and have it amended as appropriate.

Note: In certain situations, PCCU may not be able to provide access to all the personal information it holds about a member.

Exceptions to the access requirement will be limited and specific.

The reasons for denying access include, but are not limited to 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 institution for the purposes of enforcing any law of Canada, a province or a foreign jurisdiction, carrying 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 member;
- providing access could reasonably be expected to threaten the life or security of another person, provided this information cannot be severed from the file containing other information requested by the member;
- the information was collected without the knowledge or consent of the member 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.

9.1 Upon request, PCCU will inform a member of the existence, use, disclosure, and source of personal information about the member held by PCCU, and will allow the member access to this information. However, PCCU may choose to make sensitive medical information available through a medical practitioner.

9.2 For PCCU to provide an account of the existence, use, and disclosure of personal information it holds, a member may be asked to provide sufficient information to aid in the search. The additional information provided will only be used for this purpose.

9.3 In providing an account of third parties to which it has, or may have, disclosed personal information about a member, PCCU will be as specific as possible, including a list of third parties.

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

9.5 When a member successfully demonstrates the inaccuracy or incompleteness of personal information, PCCU will 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 will be transmitted to third parties having access to the information in question.

9.6 When a challenge is not resolved to the satisfaction of a member, the substance of the unresolved challenge will be recorded by PCCU. When appropriate, the existence of the unresolved challenge will be transmitted to third parties having access to the information in question.

Principle 10 – Challenging Compliance

10.0 A member will be able to question compliance with the above principles to PCCU's Privacy Officer. PCCU will have policies and procedures in place to respond to a member's questions and concerns.

10.1 The name of the Privacy Officer will be known to staff and identified to members periodically.

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

10.3 Members that make inquiries or lodge complaints will be informed by PCCU of the existence of relevant complaint procedures. PCCU will also inform member of their right to file a complaint with the Privacy Commissioner of Canada.

10.4 PCCU will investigate all complaints. If a complaint is found to be justified, PCCU will take appropriate measures, including revision of the personal information and, if necessary, amending PCCU's policies and procedures.

Principle 11 – Breach Notification, Reporting and Record Keeping

11.0 PCCU will determine if a breach of security safeguards creates a real risk of significant harm

11.1 PCCU will report to the Privacy Commissioner any breach of security safeguards that result in a real risk of significant harm.

11.2 PCCU will notify affected individuals of any breach of security safeguards that result in a real risk of significant harm.

11.3 PCCU will notify any other organization or government institution of the breach in order to reduce the risk of harm.

11.4 PCCU will keep records of every breach in security safeguards involving personal information under its control.