Auto Workers Community Credit Union

Credit Union Board of Directors Introduction, Resolution and Code for the Protection of Personal Information

INTRODUCTION

Privacy legislation establishes legal privacy rights for individuals and sets enforceable obligations for business organizations to protect personally identifiable information collected, used or disclosed for commercial purposes. With some limited exceptions, information about an identifiable person can only be collected, used or disclosed with the person's knowledge and consent.

The Code, is modeled after the ten principles of the CSA Model Code, which forms the basis for privacy compliance and reflects Credit Union limitations and differences.

DEFINITIONS AND CREDIT UNION CODE

Auto Workers Community Credit Union has adopted the Credit Union Code for the Protection of Personal Information (the Code) effective January 1, 2004. The requirements of the Code establish the credit union's operational use of personal information as well as use of employee information.

The following definitions and ten interrelated privacy principles are derived from the Code specified in the Personal Information Protection and Electronic Documents Act, and form the basis of the Code:

DEFINITIONS

"collection" means the act of gathering, acquiring, or obtaining personal information from any source, including third parties.

"consent" means voluntary agreement to the collection, use and disclosure of personal information for specified purposes. Consent may be express or implied. Express consent can be given orally or in writing, it is unequivocal and does not require any inference on the part of the Credit Union. Implied consent exists when the Credit Union can reasonably infer consent based upon your action or inaction.

"disclosure" means making personal information available to a third party.

"personal information" means information about an identifiable individual but does not include business contact information of an individual. Personal information does not include information that is about corporate or commercial entities. It also does not include information that cannot be associated with a specific individual.

"PIPED" means the Ontario Personal Information Protection and Electronic Documents Act 2000, c.5

"Third Party" means an individual or organization other than The Credit Union or Member.

"Privacy Officer" means an individual designated by The Credit Union who is accountable for The Credit Union's compliance with this Policy and who can be contacted as set out at the end of this Policy.

"use" means the treatment and handling of personal information by and within the Credit Union.

INTERRELATED PRIVACY PRINCIPLES

Principle 1 - Accountability

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

As such, the Credit Union Board of Directors are ultimately accountable for credit union compliance with the Code, the creation and review of all Board policies specific to the Code and the designation of the Credit Union Privacy/Deputy Privacy Officers.

Privacy Officer

The Board of Directors will designate a Privacy Officer, in consultation with the CEO/General Manager, who has primary day-to-day responsibility for compliance with the Code. The Board of Directors will notify all employees in writing of the appointment.

The Privacy Officer appointed by the Board of Directors is a senior manager within the credit union who does not have a potential conflict of interest over any aspects of personal information protection such as marketing, sales, human resources or responsibility for technical safeguards.

Other individuals within the credit union, are accountable for the day-to-day collection and processing of personal information, or to act on behalf of the Privacy Officer. It is the responsibility of the Privacy Officer to ensure employees are adequately trained in order to understand and follow all Privacy policies and procedures.

Deputy Privacy Officer

The Board of Directors will designate, in consultation with the CEO/General Manager, a substitute senior manager who will be available in the event of absences by the primary Privacy Officer and will have identical decision-making responsibilities during those absences.

Third Party Accountability

A credit union is considered to have control of any personal information that has been collected by, is in the custody or possession of, and/or is used within the credit union, including information that has been transferred to a Third Party for processing purposes.

The credit union will use contractual or other means to provide a comparable level of protection while the information is being processed by a Third Party.

BOARD REPORTING AND NOTIFICATION

Quarterly Reporting

The Privacy Officer will continually review the Code and its compliance within the credit union and will report to the Board of Directors and/or senior management any matters concerning non-compliance with the credit union's Code principles, policies or procedures that are likely to require input from the Board. The Privacy Officer will prepare a Quarterly Report for the Board that identifies key activities.

Annual Reporting

The Privacy Officer will prepare an Annual Review of the effectiveness of the Board policies to ensure compliance with the Code and to recommend any revisions as deemed appropriated. This report is due within four months of the end of each calendar year.

Principle 2 – Identifying Purposes

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

Approval, Documentation of Purposes, Member and Employee Disclosure

The Privacy Officer will document all purposes for which personal information is collected, used or disclosed including existing and new purposes. All new purposes must be, approved by the Privacy Officer prior to collection of information for the new purpose.

If the proposed purpose is significantly different than existing purposes or involves a new disclosure to a Third Party, the proposed purpose must be, approved by the Board of Directors prior to implementation.

Member/Employee Disclosure

The Credit Union will make reasonable efforts to ensure that Members/Employees are aware of the purpose(s) for which their personal information or Employee information is collected, including any disclosure of their personal information to Third Parties. The primary communication method will be the use of written or electronic statements on applications, forms, contracts and agreements.

The following collections, uses and disclosures are a necessary part of Member/Employee relations with the Credit Union:

- to provide and administer products and services requested and to use/disclose the information for any purpose related to the operation of accounts and the provision of requested products and services;
- to determine your financial situation including obtaining credit reports;
- to provide information to third party suppliers of products and services, such as data service providers, cheque printers, card manufacturers, etc.;
- to provide the information to credit bureaus and other financial institutions to update credit information;
- to protect the Credit Union, Member and others from fraud and error and to safeguard the financial interests of the Credit Union;
- to authenticate Member identity;
- to provide information to anyone working with or for the Credit Union as needed for the operation of an account or the provision of requested products and services;
- to collect debts owed to the Credit Union;
- to manage or transfer assets or liabilities of the Credit Union, such as in the case of acquisitions and mergers, loans syndications and securitizations or sales of mortgages; and
- to comply with legal and regulatory requirements

Other uses:

- The Credit Union may use the Member's personal information to offer additional or alternative services to the Member and may add it to client lists which they prepare and use for this purpose;

- The Credit Union may share personal information with authorized suppliers and agents which may offer their services to you;

- The Credit Union may use a Member's social insurance number as an aid to identify the Member with credit bureaus and other financial institutions for credit history file matching purposes;

- The Credit Union may contact you for survey purposes.

The Credit Union is required by law to obtain the Member's social insurance number to report interest on deposits and dividends on shares and other investment income to Canada Customs & Revenue Agency.

The Member may instruct the Credit Union to refrain from using or sharing information in the four ways described above at any time by providing written notification to the Credit Union's Privacy Officer. The Credit Union acknowledges that the sharing of information in the four ways described above is at the Member's option and that a Member will not be refused credit or services merely because you advised the Credit Union to stop using or sharing information in these ways. See last paragraph in Principle 3 - Consent

Principle 3 – Consent

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 the Code.

Further consent will not be required when personal information is supplied to agents of the credit union who carry out functions such as data processing, credit bureaus, cheque printing and cheque processing.

The credit union Privacy Officer must authorize all instances where a member's information is collected, used or disclosure without the member's knowledge and consent. Such instances are described in the Credit Union Code for the Protection of Personal Information and the Privacy Officer Procedures Manual.

Obtaining Consent

The Credit Union will obtain the Member's consent to collect, use or disclose personal information except where the Credit Union is authorized or required by PIPED Act or other law to do so without consent. For example, the Credit Union may collect, use or disclose personal information without the Member's knowledge or consent where:

- The Credit Union is collecting or paying a debt; or

- The Credit Union is obtaining legal advice; or

- The Credit Union reasonably expects that obtaining consent would compromise an investigation or proceeding; or

- The Credit Union is obtaining information under circumstances where a person is seriously ill or mentally incapacitated.

Consent can be expressed, implied or given through an authorized representative such as a lawyer, agent or broker. The Privacy Officer must review and approve all methods of obtaining consent.

Consent Limits on Information Collection

The credit union 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.

Where additional information that is non-essential to the product or service is sought from members, this shall be collected only as optional information, at the discretion of the member.

Refusal to provide this optional information will not influence the member's consideration for a product or service.

The Privacy Officer will review the personal information requirements of all products or services to ensure that only information required for the legitimate purpose is collected and used.

Withdrawing Consent

The credit union will obtain a written request (signed and dated) from a member who seeks to withdraw consent. The written request must acknowledge that the member has been advised that the credit union may subsequently not be able to provide the member with a related product, service or information that could be of value to the member.

The withdrawal of consent is subject to any legal or contractual restrictions that the credit union may have with the member or other organizations such as: the Income Tax Act; credit reporting; or to fulfill other fiduciary and legal responsibilities.

Principle 4 - Limiting Collection

The collection of personal information will be limited to that which is necessary for the purposes identified by the credit union. Information will be collected by fair and lawful means, and not by misleading or deceiving members about the purpose for which information is being collected.

The credit union will not collect personal information indiscriminately. It 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 these policies.

The Credit Union will limit collection of information to that which is reasonable and necessary to provide a product or service and which is reasonable and necessary for the purposes consented to by the Member. The Credit Union will also collect information as authorized by PIPED Act or other law.

The Credit Union will not collect personal information indiscriminately. It 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 these policies.

Principle 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 Member or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.

Safeguard Standards

The Credit Union shall protect the interests of its Member(s) 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 Party suppliers is strictly limited to programs endorsed by the Credit Union. As well, the Privacy Officer must be satisfied that the personal information is adequately safeguarded by the Third Party.

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

Retention of Personal Information

The Privacy Officer will ensure that guidelines and procedures with respect to the retention of personal information are maintained within the Credit Union. These guidelines will include minimum and maximum retention periods and will conform to any legislative requirements.

Destruction of Personal Information

Subject to any legislative requirement to retain records, personal information that is no longer required to fulfill the identified purposes will be destroyed, erased, or made anonymous. The Privacy Officer will ensure that the Credit Union has guidelines and procedures to govern the destruction of personal information.

Principle 6 - Accuracy

The Privacy Officer will ensure that the Credit Union has guidelines and procedures to ensure that member data it collects or generates directly is as accurate, complete and up-to-date as is necessary. 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.

If a Member demonstrates the inaccuracy or incompleteness of personal information, the Credit Union will amend the information as required. If appropriate, the Credit Union will send the amended information to third parties to whom the information has been disclosed.

When a challenge regarding the accuracy of personal information is not resolved to the Member's satisfaction, the Credit Union will annotate the personal information under its control with a note that the correction was requested but not made. See Principle 10 – Challenging Compliance

Principle 7 - Safeguarding Personal Information

Personal Information shall be, protected by security safeguards appropriate to the sensitivity of the information. The Credit Union will apply the same standard of care as it applies to safeguard its own confidential information of a similar nature.

Credit Union Safeguards

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

The Privacy Officer will conduct regular audits of organizational practices related to the safeguarding of personal information.

The Privacy Officer will periodically remind, Employees, Officers and Directors of the importance of maintaining the security and confidentially of personal information.

Employees, Officers, and Directors are required to sign an Oath of Ethical Conduct annually, including commitment to keep Member's personal information secure and strictly confidential.

Third Party Agents/Suppliers Safeguards

Third Party Agents or Suppliers are required to safeguard personal information disclosed to them in a manner consistent with the policies of the Credit Union. Examples include data processors, credit bureaus, cheque printers and cheque processors.

The Privacy Officer will collaborate with third parties specializing in security safeguards, as required, to ensure the required level of protection. To achieve a comparable level of protection The Credit Union and Third Parties sign a formal agreement to safeguard personal information.

The Credit Union will not enter into any commercial relationships with organizations that do not agree to abide by acceptable limitations on information uses and appropriate safeguards.

Destruction of Personal Information Safeguards

The Credit Union will dispose of or destroy personal information in a secure manner to prevent any unauthorized access. Acting upon the Inactive Records Retention and Destruction Policy the Privacy Officer will oversee;

1. The proper and orderly storage of all archived documents in their respective area(s).
2. Undertake an annual review of archived records to identify documents that are redundant consistent with the Inactive Record Retention Schedule;
3. Issue a Destruction Notification; a general letter or detailed listing announcing the scheduled destruction of a department's records.

E-Mail

Confidentiality and security are not assured when information is transmitted through e-mail or other wireless communication. The Credit Union will not be responsible for any loss or damage suffered as a result of a breach of security and/or confidentiality when you transmit information to The Credit Union by e-mail or other wireless communication or when the Credit Union transmits such information by such means at your request.

Principle 8 - Openness

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

This can be accomplished through the use of brochures, information sheets, online Web information, etc., and must include the following information:

- The name or title and the address of the Privacy Officer who is accountable for the compliance with the Credit Union's policies and procedures and to whom complaints or inquires can be directed;
- The means of gaining access to personal information held by the Credit Union;
- A description of the type of personal information held at the Credit Union, including a general account of its use; and
- The types of personal information made available to related organizations such as subsidiaries or other suppliers of services.

The Privacy Officer will review the methods of dissemination, and the form in which the information is presented to ensure, that it is easy to locate, understandable and accessible.

Principle 9 - Individual Access

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

All access requests must be submitted in writing and include adequate proof of the individual's identity or right to access, and sufficient information to allow the Credit Union to locate the requested information.

Member information, such as copies of statements, transaction slips and account agreements will be provided upon request and authentication of identity.

Restricting Access

In certain situations, the Credit Union 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 and include the following:

1. Providing access would reveal personal information about a Third Party;
2. The personal information to which the Member has requested access has been requested by a government institution for the purposes of enforcing the laws, carrying out an investigation related to the enforcement of any law, the administration of any law, the protection of national security and the defense of Canada or the conduct of international affairs;
3. The information is protected by solicitor-client privilege;
4. Providing access would reveal confidential commercial information;
5. Providing access might threaten the life or security of another individual;
6. The information was collected without knowledge or consent for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province; or
7. The information was generated in the course of a formal dispute resolution process.

The Privacy Officer must be made aware of any situations involving Employees, Members or other individuals that would result in legal restrictions on access.

Treatment of Opinions and Judgments

The Credit Union cannot withhold from a Member any opinions and judgments formed about the Member as a basis for determining their eligibility for any products and services. The Credit Union will provide a Member, upon written request, access to all information that may have been used in making a determination about a Member's eligibility for service, other than in the specific restriction mentioned above in Restricting Access.

Timeframe for Response

The Credit Union shall respond to a Member's request within 30 days. This timeframe can be expanded, only if required, and upon written notification to the Member.

Cost of Response

At the Privacy Officer's discretion, the Credit Union may impose a fee at a stated hourly rate where collection of the requested information requires exceptional time and effort. The Member must be informed of an estimate of costs prior to the commencement of the request.

Principle 10 - Challenging Compliance

Any individual can challenge the Credit Union's compliance with any of the Code principles. The Privacy Officer is accountable for the Credit Union's Compliance and shall investigate all complaints. Accordingly, the Privacy Officer shall, be known to Members, Staff, Officers, and Directors.

Inquiry and Complaint Handling Process

The Privacy Officer will create and maintain documented procedures to respond to a Member, Employee, Officer, or Board of Director's questions or concerns. These procedures must be readily accessible to Credit Union Members, Employees, Officers and Board of Directors.

Inquiries and complaints must be in writing, with a formal process in place to receive and track them and the Credit Union must respond as quickly as possible within 30 days.

Required Measures for Justified Complaints

The Privacy Officer is responsible for ensuring appropriate measures are taken when a complaint is found to be justified. These measures will include:

1. Written response to be complainant within the specified timeframe of 30 days;
2. Revision of the challenged personal information;
3. If required, revision to policies and procedures;
4. Review of any complaint that requires disciplinary action against a Credit Union Employee with the appropriate Manager(s);
5. Reporting of the non-compliance to the Board of Directors, including the actions proposed or taken to resolve the issue, as specified in Principle -1- Board Reporting and Notification.

CONTACT INFORMATION:

Privacy Officer
The Credit Union
P.O. Box 158
Oshawa,Ontario
L1H 7L1