Privacy Policy

UV INSURANCE

Table of Contents

1. Purpose of Policy

At The Union Life Mutual Assurance Company (hereinafter "UV Insurance"), we are committed to protecting the privacy of our clients, employees and agents, and to ensuring the confidentiality of the personal information provided to us in the course of our business.

Our Privacy Policy not only meets the requirements of the *Act respecting the protection of personal information in the private sector*[1] (hereinafter "ARPPIPS") and *The Personal Information Protection and Electronic Documents Act* (hereinafter "federal privacy law")[2] but also describes our standards for collecting, using, disclosing and retaining your personal information. This Policy also explains how we safeguard your personal information and your right to access that information.

This document is updated on an ongoing basis to ensure that you are aware of changes to our privacy practices, and to unify these practices and comply with the applicable legislation. We encourage you to review this Policy regularly for updates.

2. Scope

Drawing on industry best practices, UV Insurance affirms its commitment to comply with the laws and regulations governing privacy and to protect all confidential information in its possession. All UV Insurance employees who collect, use or disclose personal information are required to adhere to this Policy. The Board of Directors of UV Insurance is also subject to this policy.

A violation of this policy may result in significant disciplinary action depending on the negligence or intentional nature of the misconduct.

UV Insurance's responsibility for privacy also extends to its agents, service providers and partners who offer the same high level of protection to your personal information. While UV Insurance does not expect this policy to apply directly to its suppliers or business partners, it does expect that a due diligence analysis will be conducted with its suppliers and partners to ensure that they have adequate privacy controls in place. These safeguards take into account information technology and cybersecurity risks. This due diligence analysis is included in the outsourcing risk management program. Our commitment to the fair treatment of customers and the protection of their personal information extends to services outsourced to our service providers and business partners.

[1] *Act respecting the protection of personal information in the private sector*, CQLR, c. P-39.1.
[2] *Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5).*

3. Personal Information

Personal information is any information about an individual that identifies him or her, such as financial, lifestyle or health information.[3] Personal information is confidential, meaning that it cannot be disclosed without the consent of the individual concerned.

Personal information must be protected regardless of its characteristics or its form, whether written, graphic, audio, visual, computerized or any other form.

4. Purpose of Information Collection

UV Insurance must collect information about you in order to provide you with high quality services. The nature and sensitivity of the information we collect about you varies depending on the services we provide and the legal requirements we must comply with. Some examples include:

- Name, address, email and phone number;
- Age, gender, marital status, family status;
- Identification numbers such as your driver's license number or social insurance number;
- Your insurance coverage, transaction and service usage history;
- Financial information, such as your place of employment, sources of income, credit history, assets and liabilities;
- Medical information, if required for some of our insurance products;
- Your social insurance number if a selected product generates investment income[4].

The purposes for which we collect information are usually to provide you with the products or services you have requested from us, confirm your identity, estimate insurance risks, determine your premium, process your claims, meet legal requirements, prevent fraud, or resolve issues regarding our relationship.

The purposes for which we collect your personal information are identified at or before the time of collection. For example, information is collected when you submit an application, open an account or make a claim.

Customer service calls may be monitored and recorded for accuracy, training or quality of service purposes.

[3] Section 1, ARPPIPS, CQLR, c. P-39.1.
[4] Section 4, ARPPIPS, CQLR, c. P-39.1.

5. Consent

When we collect personal information about you, we obtain your consent to use it for the purposes for which it was collected. UV Insurance requires your consent to use your information for any other purposes or to collect additional information about you. This consent may be obtained in writing, verbally, electronically or through an authorized representative, such as your financial security advisor. If you do not consent to the collection, use and sharing of your personal information, we may not be able to provide you with the products and services you have requested or the administration of your file may be compromised.

As a general rule, we require your express written consent to collect[5], use or disclose your personal information. When less sensitive information is involved, we may, under certain circumstances, accept your verbal consent. Occasionally, we may imply consent where it can be inferred from your action or inaction.

Consent must be given by you or your authorized representative such as a legal guardian or a person having power of attorney.

You may withdraw your consent at any time, subject to legal or contractual restrictions. For example, your right to withdraw your consent is necessarily limited where we need information to extend a loan against the value of a policy issued by us. We will inform you of the consequences of withdrawing consent, including the possibility that we may be unable to provide a product or process your request. If you choose to withdraw your consent, we will document our records accordingly. We ensure that the records we have are up to date and accurate when they are used.[6]

Under certain circumstances, we may be required or obligated to collect, use or disclose personal information without your consent. This occurs when legal, medical or security reasons may make it impossible or difficult to obtain consent[7]. Where information is collected to investigate a possible breach of contract, to prevent or detect fraud, or to enforce the law, obtaining consent may be detrimental to the purpose for which the information is collected. In some cases, obtaining consent may be impossible or inappropriate if you are a minor, seriously ill or incapacitated.

6. Limits to Collection, Use and Disclosure

We limit the collection of your personal information to what is necessary for the purposes explained to you.[8] We collect personal information directly from you, unless you allow us to collect this information from a third party or we have legal authority to do so[9].

We limit the use of your personal information to the purposes for which it was collected. This means that we cannot use your personal information for any other purpose without your consent, except as required by law.

[5] Section 14, ARPPIPS, CQLR, P-39.1.
[6] Section 11, ARPPIPS, CQLR, P-39.1.
[7] Sections 18 to 23, ARPPIPS, CQLR, P-39.1.
[8] Section 5, ARPPIPS, CQLR, P-39.1.
[9] Section 6, ARPPIPS, CQLR, P-39.1.

When necessary, and only with your consent or where permitted by law, we may disclose your personal information to certain authorized parties for the proper management of your contract or to meet regulatory and/or legal requirements, including:

- Your financial security advisor and his or her employees and any agency with whom we do business and who have the right to supervise, directly or indirectly, your advisor and his or her employees;
- Any person or organization to whom you give your consent;
- Reinsurers;
- Service providers and agents who need the information to fulfill their contract or mandate and ensure the proper administration of our products;[10]
- Legal or judicial authorities, where required by law, for example in the case of fraud or criminal activity.

Notwithstanding the foregoing, your personal information is accessible only to authorized persons, and only to the extent necessary to perform their duties.

You have the right to know, upon request, to whom your information has been disclosed. We will refuse to disclose this information only in exceptional circumstances and in accordance with the law. We maintain accurate records of the persons to whom we have disclosed your information and the circumstances under which your information was disclosed.

We may, under certain circumstances, use service providers outside Canada, including the United States. We are responsible for the service providers' compliance with our Privacy Policy and will ensure that their level of protection of personal information is comparable to our own.

7. Retention

We retain your personal information as long as needed for the purpose for which it was collected. We must destroy, erase or make anonymous this information in accordance with the law[11]. At all times, employees shall take the security measures that are needed to ensure the protection of personal information collected, used, disclosed, retained or destroyed and that are reasonable given the sensitivity of the information, the purposes for which it is to be used, the quantity and distribution of the information and the medium on which it is stored.

When we destroy your personal information, we make sure that its confidentiality is safeguarded and that no unauthorized person can access it during the destruction process.

We may de-identify personal information. This process removes the link between the information and your identity to protect it once the purposes for which the information was retained have been achieved.

[10] These service providers or agents undertake to comply with privacy legislation before any personal information is provided to them.
[11] Sections 10 and 12, ARPPIPS, CQLR, P-39.1.

8. Use of Personal Information for Promotional Purposes

In order to offer you, from time to time, products and services that may meet your needs, send you special offers and advice, and better serve you, UV Insurance may use the contact information you provided (name, address, phone number, email address, etc.) to contact you and may share a list of its clients' contact information with other companies that make up UV Insurance. You may withdraw your consent at any time by contacting us. This does not include communications about the product you own or administrative communications necessary for the proper management of your file.

In order to satisfy legal requirements, we must obtain your consent before allowing the companies that make up UV Insurance to use and share your personal information for promotional purposes, to the height of your expectations.

Your information will be used so that we can offer you a personalized experience and, from time to time, send you information, offers and advice tailored to your personal situation and interests. UV Insurance will not share your information with other companies without obtaining your prior consent or unless permitted by law.

We will never use sensitive personal information for promotional purposes without first obtaining your specific consent.

You may ask us at any time not to use or share your personal information with the companies that make up UV Insurance for promotional purposes by sending a written request to the Privacy Officer at the address indicated at the end of this document.

If you do not consent to the collection, use and sharing of your personal information, we may be unable to provide you with the requested products and services to the height of your expectations.

Please note that we do not sell our client lists to third parties.

9. Accuracy and Accountability

We make every possible effort to ensure that your personal information is as accurate and complete as necessary for the purposes for which it is collected, used or disclosed.

We are responsible for personal information in our possession or custody, including information that we entrust to third parties for processing. We require such third parties to keep personal information under strict standards of privacy and protection. We provide access to personal information only to those individuals within the company who are qualified to receive such access, where such information is necessary for the performance of their duties.

We adhere to legislated and self-imposed rules, aimed to safeguard your privacy. These rules are set out in this Privacy Policy, the UV Insurance Code of Ethics (applicable to directors, officers and employees) as well as insurance industry guidelines and other applicable legislation. Our staff is informed and adequately trained on our privacy policies and practices.

10. Security Safeguards

We have implemented and continue to develop rigorous safeguards to ensure that your personal information remains strictly confidential and is protected against loss or theft and from unauthorized access, disclosure, copying, use or modification.

These safeguards include:

- Organizational measures (e.g. use of security clearances, limiting access to a “need-to-know” basis, a cybersecurity department, policies, guidelines and compliance training);
- Physical measures (e.g. electronically managed access to offices for employees, off-site back-ups and archiving, etc.);
- Technological measures (e.g. use of passwords and encryption, frequent password changes, use of firewalls and segmented operator access, etc.).

UV Insurance expects its employees to demonstrate transparency and accountability by reporting any breaches of privacy obligations to their manager and the Chief Compliance Officer.

We recommend that you use unique and strong passwords for your online accounts and not share your passwords with anyone.

11. Request for Access or Change to Your Personal Information

You have the right to know whether we have personal information about you and to inspect that information. You also have the right to enquire how we collected your personal information, how we used it, and to whom it may have been disclosed. The request is addressed to the UV Insurance Privacy Officer[12].

This information will be provided to you within a reasonable time from the date we receive your written request[13].

In certain specific circumstances, we may refuse to provide you with the requested information. Exceptions to your right of access may include:

- Requested information that would be prohibitively costly to provide;
- Information that contains references to other individuals;
- Information that cannot be disclosed for legal, security or commercial proprietary reasons;
- Information that was obtained in the course of an investigation into a possible breach of contract or to prevent or detect fraud;
- Information that is subject to solicitor-client or litigation privilege.

When we have medical information about you, we may refuse to provide it directly to you and request that it be given to a health care professional you designate to provide it to you.

In some cases, we may not be able to provide you with access to all the information we have about you. There may be a fee for the request for personal information you submit. We will inform you of any such fees.

[12] Sections 30 paragraph 2, ARPPIPS, CQLR, P-39.1.
[13] Sections 32 paragraph 2, ARPPIPS, CQLR, P-39.1.

You may verify the accuracy and completeness of your personal information and, if appropriate, request a correction. We will respond to any request for correction within thirty (30) days of receipt of the written request. All requests for access to information should be sent to the address at the end of this policy.

Any refusal by UV Insurance to grant a request will be explained to you in writing and will indicate the provision of the law on which our refusal is based and the recourse available to you. The time limit within which your recourse may be exercised will also be indicated. UV Assurance will also provide assistance to help you understand the denial[14].

12. Confidentiality Incident

A confidentiality incident means:

- Access not authorized by law to personal information;
- Use not authorized by law of personal information;
- Release not authorized by law of personal information;
- Loss of personal information or any other breach of the protection of such information.

A confidentiality incident may occur as a result of a breach of UV Insurance security measures. For example, the incident may be the result of simple human error or negligence, or it may be a failure to implement and enforce security measures[15].

An operational incident, on the other hand, is defined as an event that causes or is likely to cause a disruption, slowdown or interruption of UV Insurance's critical activities and that could result in financial loss or damage to reputation.

That said, a confidentiality incident that would result in financial loss or damage to UV Insurance's reputation is considered an operational incident.

In the event of a confidentiality or operational incident, UV Insurance follows a series of steps to protect the personal information of its clients and limit the consequences. As UV Insurance is a company offering products in several Canadian provinces, we make sure to apply the highest regulatory standards.

Preliminary Assessment

The manager of the department involved in the incident completes a confidentiality incident report (for internal use). If information is not yet available at the time of reporting the events, the manager must indicate that "information is not yet available" and agree to provide it as soon as possible.

[14] Sections 34 paragraph 2, ARPPIPS, CQLR, P-39.1.
[15] A confidentiality incident may take many forms, for example: Computer intrusion into servers by unauthorized internal or third parties, phishing, malware deployment, ransomware attacks, botnets, brute force attack, sending an email to the wrong recipient, loss of data caused by a virus, loss or theft of paper or electronic documents containing personal information, loss of a cell phone or laptop, a computer breach or human error, unauthorized access, retrieval or disclosure of personal information, etc.

Privacy Officer

UV Insurance has a Privacy Officer[16] who ensures compliance with privacy legislation[17] and plays a role in:

- Establishing and implementing policies and practices for governance of personal information and ensuring the protection of such information[18];
- Conducting privacy impact assessments (PIAs)[19];
- Reporting any communication likely to reduce the harm caused by a confidentiality incident and the assessment of the harm caused by that incident[20].

Privacy Officer
privacy@uvinsurance.ca
1990 Jean-Berchmans-Michaud St.
Drummondville QC J2C 7G7
Telephone: 819-478-1315
Toll Free: 1-800-567-0988
Fax: 819-474-1990

Notice

Following this report, an assessment is conducted by senior management and the Privacy Officer to determine whether the incident presents a risk of serious harm[21]. If so, UV Insurance will promptly report the incident to the provincial or federal privacy commissioner[22].

When UV Insurance determines that a confidentiality incident meets the definition of an operational incident mentioned above, it shall notify the Autorité des Marchés Financiers as soon as possible, or no later than 24 hours after determining that the incident is considered “operational.”

In addition, UV Insurance must also notify:

- Any person whose personal information is involved in the incident; and
- Any person or organization that may be able to mitigate this risk (by providing only the information necessary for this purpose).

Containing a Privacy Breach

Following the preliminary assessment, UV Insurance takes all reasonable steps to reduce the risk of harm. That said, immediate action is take across the organization to limit the consequences of unauthorized access, use or disclosure, loss or theft of personal information by ensuring that the non-compliant practice, if any, is stopped.

[16] Section 3.1, ARPPIPS, CQLR, c. P-39.1.
[17] Section 3.1 paragraph 2, ARPPIPS, CQLR, c. P-39.1.
[18] Section 3.2 paragraph 1, ARPPIPS, CQLR, c. P-39.1.
[19] Section 3.3 paragraph 2, ARPPIPS, CQLR, c. P-39.1.
[20] Section 3.5 paragraph 2, ARPPIPS, CQLR, c. P-39.1.
[21] Section 3.7, ARPPIPS, CQLR, c. P-39.1.
[22] Section 3.5, ARPPIPS, CQLR, c. P-39.1.

Confidentiality Incident Register

The incident must be recorded in the UV Insurance's confidentiality incident register, even if there is no risk of serious harm[23]. To do so, the Privacy Officer uses the compliance tool to assign the prescribed form to the affected manager, who completes and submits it.

The Privacy Officer then analyzes the form, takes the necessary actions (if any) and records it in the register.

Comprehensive Assessment, Changes and Implementation of Corrective Measures

At this stage, the situation is investigated further so that the internal standards, policies or directives in place at the time of the incident are identified and reviewed. The purpose is to verify whether they were followed by the persons involved, and if not, identify the reasons why they were not followed. In the case of a procedural error or an operational failure, it will be documented in the file and processes will be adapted to prevent such an incident from recurring.

Depending on the type of incident and the applicable context, the Privacy Officer will have to implement reasonable measures to:

- Reduce the risk of harm being caused; and
- Prevent a similar incident from occurring in the future[24].

Reasonable measures take into account the size and complexity of the company. With the objective of preventing a similar incident from recurring, there are multiple measures possible, including the:

- Implementation of systematic controls created within the compliance tool for management personnel or specific users;
- Creation of additional procedures;
- Initiation of in-depth process investigations;
- Provision of ad hoc training.

And lastly, recommendations for medium- and long-term solutions are made and follow-up is carried out.

> Rest assured that at UV Insurance, we take the protection of our clients' personal information very seriously and we won't hesitate to implement all the necessary means to achieve this.

13. Limitation of Liability

The use of technologies such as the Internet carries substantial risk, making it impossible to guarantee that the personal information you provide is completely secure. However, rest assured that UV Insurance uses all reasonable means at its disposal to protect your data.

[23] Section 3.8, ARPPIPS, CQLR, c. P-39.1.
[24] Section 3.5, ARPPIPS, CQLR, c. P-39.1.

You therefore acknowledge that UV Insurance and its suppliers cannot be held liable for any damages or harm that may arise or result, directly or indirectly, from a privacy breach in relation to the data and/or information sent via the Internet to UV Insurance.

14. Transparency, Concerns and Complaints

Our employees can answer your questions and concerns about privacy and the protection of your personal information. To inspect your file, to make a complaint about non-compliance with privacy procedures or to obtain more information about the Privacy Policy, please contact us.

To contact us

UV INSURANCE

1990 Jean-Berchmans-Michaud St.
Drummondville (Quebec) J2C 7G7
Telephone: (819) 478-1315
Toll Free: 1-800-567-0988