CANATICS
Canadian National Insurance Crime Services

1. INTRODUCTION

Canadian National Insurance Crime Services (CANATICS) is a not-for-profit fraud consortium that works together with the Canadian insurance industry to combat organized and premeditated insurance crime in a manner that protects and respects individual privacy. This requires CANATICS to collect and pool personal information from insurance companies (referred to as "Members") to enable CANATICS to generate alerts for potentially suspicious claims, specific to each Member, which, in turn, can be further investigated by the Members.

CANATICS recognizes that having strong privacy measures and systems in place is critical to promoting the privacy interests of individuals who indirectly share their personal information, via Members, with CANATICS to achieve its mission in combatting insurance fraud for the benefit of Canadians.

In so doing, CANATICS adheres to the highest standards of data protection that respect and abide by Canadian legislative requirements, internationally recognized data protection standards and leading privacy best practices, which this Privacy Policy (the "Policy") reflects.

CANATICS is recognized by the Information Privacy Commissioner/Ontario as a Privacy Ambassador for adhering to the principles of "Privacy by Design" in its fraud analytics solution. CANATICS fraud analytics solution has also received the official Privacy by Design Certification from the Privacy and Big Data Institute at Ryerson University.

2. AUDIENCE AND SCOPE

This Policy governs the collection, use, disclosure, retention, destruction and overall protection of "personal information" in the custody or control of CANATICS.

For the purposes of this Policy, "personal information" means information about an identifiable individual, collected by CANATICS about individuals via its Members, such as name, policy, claims data, and intel (e.g. information intelligence gathered from other sources or organizations). It also includes personal information about personnel (e.g. employee related information).

Members involved in contributing personal information, are subject to, and responsible for, complying with their own governing privacy legislation, organization-specific privacy policies, procedures and guidelines for the local handling and storage of their own customer data. This Policy intends to compliment and build upon the existing privacy policies and information handling practices at each Member organization to ensure a robust privacy governance and accountability framework.

This Policy applies to all CANATICS personnel, including staff, consultants, and subcontractors involved in handling personal information.

It also applies to third party service providers, their employees and subcontractors who must comply with all applicable CANATICS policies and related procedures. As such, applicable provisions of this Policy are addressed in CANATICS' third party service agreements.

"Third party", for the purposes of this Policy, means any third party individual or organization with whom CANATICS contracts for services, including its employees and subcontractors.

3. POLICY REQUIREMENTS

3.1. Privacy Principles

CANATICS' **Privacy Policy** is organized around the ten internationally accepted fair information principles set out in the Canadian Standards Association (CSA) *Model Code for the Protection of Personal Information* (the "CSA

Model Code"), and incorporated as a Schedule into the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA).

The CSA Model Code forms the basis for Canadian privacy legislation and includes the following principles:

- Principle 1: Accountability
- Principle 2: Identifying Purposes
- Principle 3: Consent
- Principle 4: Limiting Collection
- Principle 5: Limiting Use, Disclosure and Retention
- Principle 6: Accuracy
- Principle 7: Safeguards
- Principle 8: Openness
- Principle 9: Individual Access
- Principle 10: Challenging Compliance

This Policy provides guidelines on what each of these principles means in the context of CANATICS' operations and information-handling practices.

3.2. Principle 1: Accountability

CANATICS is committed to upholding its integrity, honesty, ethical and legal conduct when handling personal information, in accordance with CANATICS' **Code of Conduct and Ethics**. CANATICS also meets these commitments through its Privacy Program, which is governed by this Policy.

In practice, this means CANATICS is responsible for ensuring the private and secure handling of personal information collected, used, retained, disclosed, disposed of and destroyed by CANATICS personnel.

It also means that CANATICS is responsible for supporting its third party service providers in meeting their legal obligations to protect personal information that the third party service providers collect on behalf of CANATICS for the provision of the fraud analytics solution and related services to CANATICS.

3.2.1. *Responsibility for Privacy Program*

Accountability for CANATICS' compliance with its Privacy Program and applicable federal and provincial privacy legislation rests with the Chief Privacy Officer (CPO), who reports directly to the CEO.

The key components of CANATICS' Privacy Program include:

- a **Privacy Governance Framework** comprised of this Policy, related policies and procedures for the protection of personal information, which are supported and endorsed by the Board of Directors via the Privacy and Risk Management Committee;
- **Employee Privacy and Security Training** as part of CANATICS' **Employee Onboarding Process** which all personnel must attend upon hire, and a refresher annually thereafter, including:
    - legally binding **Confidentiality Agreements** with personnel and all third parties with access to personal information;
    - annual **Employee Attestation** that confirms adherence with this Policy and all policies and procedures that govern CANATICS; and
- **Privacy Impact Assessments, Security Analyses or Threat Risk Assessments** (e.g. penetration testing)**,** as appropriate, on CANATICS' data holdings using third party service provider hosting environments.

3.2.2. *Privacy Officer Responsibilities*

The CPO provides (1) leadership, direction and problem resolution for CANATICS' Privacy Program and (2) recommendations with respect to privacy and confidentiality issues.

CANATICS' CPO is responsible for overseeing and monitoring compliance with the key components of CANATICS' Privacy Program, which involves formal reporting to the CEO, in addition to the Privacy and Risk Management Committee.

In carrying out the Privacy Program, the CPO is actively committed to fostering a culture of privacy and data protection at CANATICS, including to:

- Ensure all CANATICS privacy policies and related procedures are accurate and up-to-date and reflect current industry best practices and legislative updates;
- Ensure all CANATICS personnel comply with CANATICS' Privacy Program (including all policies and procedures);
- Ensure that CANATICS policies and procedures are communicated to the Members of CANATICS, privacy stakeholders (including the Privacy Commissioners) and the public;
- Ensure that mechanisms are in place and used to address privacy concerns and complaints;
- Maintain and ensure that all contracts with third parties include provisions that specify their privacy obligations to protect personal information handled or accessed during the course of their duties;
- Conduct or facilitate privacy and security assessments on all CANATICS data holdings as necessary;
- Monitor the effectiveness of the Privacy Program and ensure adequate and current privacy training and awareness;
- Report annually to the Privacy and Risk Management Committee on the status of its Privacy Program and any material matters or risks that may affect individual privacy, including the CANATICS brand; and
- Report privacy breaches to the relevant provincial or federal privacy and/or insurance authorities, in accordance with CANATICS' **Breach Management Policy**.

3.3. Principle 2: Identifying Purposes

CANATICS collects and uses personal information for purposes related to its work in identifying potentially suspicious networks and claims. This means that each Member will contribute their own identifiable customer data to CANATICS, in accordance with their privacy policies and procedures, which is then pooled and analyzed by CANATICS.

3.3.1. *Permitted Purposes*

CANATICS collects personal information indirectly from individuals, via each Member, for the purpose of facilitating insurers' investigations of potentially suspicious networks and claims through the use of analytical tools which examine insurance industry pooled data.

CANATICS also collects personal information directly from employees in order to establish, maintain and manage employment relationships between CANATICS and its personnel.

3.3.2. *Documenting Permitted Purposes - Notice*

CANATICS documents the purposes for which it collects personal information, which are made known by each Member at the time of collection, through the use of the regulated *Ontario Application for Automobile Insurance Owner's Form* (OAF-1), or the regulated *Application for Accident Benefits* (OCF-1), *Treatment and Assessment Plan* (OCF-18), *Auto Insurance Standard Invoice* (OCF-21) and *Treatment Confirmation Form* (OCF-23), that individuals and their applicable health service providers must read and sign when applying for auto insurance or accident benefits, respectively. Such purposes may also be explained to the individual applicant orally by an insurance broker or a call centre agent during the application process.

3.4. Principle 3: Consent

CANATICS collects personal information indirectly from individuals via each Member. CANATICS does so only where consent for the collection, use and disclosure of their personal information for fraud prevention purposes has been obtained via a number of mechanisms.

The OAF-1, OCF-1, OCF-18, OCF-21, OCF-23 forms expressly state and clarify that individuals who apply for automobile insurance or accident benefits, respectively, expressly consent to the collection and disclosure of their personal information or personal health information for the limited purpose of preventing, detecting or suppressing fraud. Individuals also expressly consent to the sharing of their personal information with fraud prevention organizations, other insurance companies, the police and databases or registers used by the insurance industry to analyze and check information provided against existing information.

Such consent is given voluntarily and without manipulation, undue influence or coercion.

3.5. Principle 4: Limiting Collection

CANATICS only collects personal information from each Member that is required for the purposes identified in this Policy, using fair and lawful means.

3.6. Principle 5: Limiting Use, Disclosure and Retention

CANATICS uses, retains and discloses personal information collected from Members in accordance with the identified and documented purpose(s) for which it was originally collected and to which the individual expressly consented, unless otherwise required or authorized by law.

3.6.1. *Need to Know – Data Minimization*

CANATICS limits the use, disclosure and retention of personal information by restricting access to a need-to-know basis for any system used by, CANATICS or its Members.

The personal information processed by CANATICS, on behalf of one Member, is not openly shared with any other Member. Members continue to own the data that they provide but do not have direct access into pooled data.

Access to information occurs through strictly controlled alerts, reports, and strictly controlled joint review of fraud data.

Access to employee-related / HR data and related handling is limited to the CEO, his delegate, and the Governance and HR Committee or any Committee of the Board of Directors as necessary for hiring and/or performance evaluation purposes.

3.6.2. *Retention and Destruction*

Personal information collected by CANATICS is retained only as long as necessary to fulfill the identified and documented purpose(s) for which it was collected. Policy and claims data will be retained for up to 3 years. Intel information will be retained for up to 7 years before all such information is securely destroyed. Storage media will be securely erased using leading industry software tools.

Any personal information that CANATICS no longer requires shall be securely erased and/or destroyed.

3.7. Principle 6: Accuracy

CANATICS relies on the personal information it receives from its Members to be accurate, complete and up-to-date as is necessary to fulfill the purposes for which it was originally collected.

All systems used by CANATICS have built in quality controls to ensure data integrity.

3.8. Principle 7: Safeguards

CANATICS protects all of its data holdings against loss, theft, unauthorized access, disclosure, copying, use, modification, transmittal, disposal and anticipated threats.

CANATICS uses contractual and other policy/procedural means to ensure a comparable level of protection while its third parties handle on CANATICS' behalf.

CANATICS stores all personal information in a secure data centre located in Canada.

3.8.1. *Security Safeguards*

CANATICS uses third party service providers to deliver sophisticated, state-of-the-art fraud analytics solutions.

These third party service providers use leading security best practices to protect the information they receive from CANATICS for the purposes of fraud prevention and detection, including but not limited to:

- Secure socket layer (SSL) and virtual private network (VPN) technology for remote access;
- Data encryption during transmission;
- Password protection for access to systems;
- Routing controls and firewalls to ensure security is not breached during data transmission;
- Network security (e.g. virus scanning, firewalls, deployment of secure zones, malware protection and secure system-to-system interfaces);
- Disaster recovery safeguards such as regular system backups (including storing backup tapes in a secure location) and maintaining system capacity;
- Access controls and reporting of user access and privilege levels;
- Audit functionality that captures all end-user activity, including the identity of the accessing user;
- Maintaining detailed inventories of system hardware, software and data;
- Regular monitoring, auditing and testing for the effectiveness of all CANATICS technical safeguards; and
- Regular monitoring and review of new and emerging technologies that could protect against new and emerging threats.

3.9. Principle 8: Openness

CANATICS makes information about its collection, use and disclosure of personal information available to the public. This Policy, including how to contact the CPO, is available for download at the following website address www.canatics.ca

3.10. Principle 9: Individual Access

CANATICS and its Members value the rights of individuals to access their personal information. Since CANATICS is a third party service provider to its Members, individuals should submit their access requests directly to the Member who is the original data collector of the individuals' personal information.

3.11. Principle 10: Challenging Compliance

Any individual may submit a concern, question or complaint to the Member who originally collected their personal information. That Member will forward the complaint where it pertains to CANATICS.

If a complaint is found to be justified, CANATICS will take appropriate measures, including, if necessary, amending its policies and procedures.

In the event that CANATICS is not able to resolve a concern or complaint, all individuals have the right to contact the Office of the Privacy Commissioner of Canada as follows:

Office of the Privacy Commissioner of Canada
30 Victoria Street
Gatineau, Quebec
K1A 1H3
Toll-free: 1-800-282-1376
Phone: (819) 994-5444
Fax: (819) 994-5424
TTY: (819) 994-6591

4. CONTACT US

If you have any questions or concerns about our privacy practices, please feel free to contact:
Privacy “@” Canatics.ca