

IT102   
Privacy Policy and Operating Manual

|  |  |
| --- | --- |
| Status | Final |
| Version | 2.03 |
| Classification | Confidential |
| Owner | Razvan Anghelidi, Directory of IT |
| Address | 1705 Tech Avenue, Unit 3, Mississauga, ON, L4W 0A2, Canada |

*Statement of Confidentiality: This document and supporting materials contain confidential and proprietary business information of Signifi Solutions Inc. These materials may be printed or photocopied for use internally and must not be shared with other parties.*

[Document Control iii](#_Toc32940213)

[Introduction 4](#_Toc32940214)

[Purpose 4](#_Toc32940215)

[Audience 4](#_Toc32940216)

[Information Privacy Program 5](#_Toc32940217)

[The Ten Principles of PIPEDA Summarized 6](#_Toc32940218)

[Definitions 7](#_Toc32940219)

[Collection of Personal Information: 8](#_Toc32940220)

[Use of Personal Information 8](#_Toc32940221)

[Disclosure of Personal Information 9](#_Toc32940222)

[Consent 10](#_Toc32940223)

[Limiting Collection 10](#_Toc32940224)

[Accuracy 11](#_Toc32940225)

[Safeguards 11](#_Toc32940226)

[Openness 12](#_Toc32940227)

[Individual Access 12](#_Toc32940228)

[Complaints/Recourse 12](#_Toc32940229)

[Policy Compliance 13](#_Toc32940230)

[Exceptions 13](#_Toc32940231)

[Non-Compliance 13](#_Toc32940232)

[Questions/Access Request/Complaint 14](#_Toc32940233)

[Data Controller Responsibilities 14](#_Toc32940234)

[Enforcement 17](#_Toc32940235)

[Revision History 17](#_Toc32940236)

All rights reserved

No part of this document may be reproduced in any form, including photocopying or transmission electronically to any computer, without prior written consent of Signifi Solutions Inc (from now on, Signifi). The information contained in this document is proprietary to Signifi and may not be used or disclosed except as expressly authorized in writing by Signifi.

Trademarks

Other product names mentioned in this document may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Document Control

The electronic version of this document is recognized as the only valid version.

Approval History

|  |  |  |
| --- | --- | --- |
| APPROVER(S) | TITLE/DEPARTMENT | APPROVED DATE |
| Shamira Jaffer | CEO | December 23rd, 2021 |
| Shamira Jaffer | CEO | December 7th, 2020 |
| Shamira Jaffer | CEO | December 19th, 2019 |
| Shamira Jaffer | CEO | February 18th, 2019 |
|  |  |  |
|  |  |  |

Document Sensitivity Level

Confidential

Introduction

Overview

The purpose of this Privacy Policy is to provide guidance to the leadership, employees and agents of Signifi on matters concerning the protection of privacy and compliance with privacy legislation in each jurisdiction in which Signifi conducts business.

Purpose

This privacy policy has been developed to comply with Canada’s Personal Information Protection and Electronic Documents Act ("PIPEDA"). PIPEDA sets out rules for the collection, use and disclosure of personal information in the course of commercial activity as defined in the Act.

Audience

This policy applies to all Signifi associates, part-time and temporary workers, trainees, contractors and vendors.

Information Privacy Program

Signifi shall implement an Information Privacy Program that shall include:

1. Privacy and security awareness training for employees and contractors of Signifi.
2. Ensuring that all agents of Signifi who have access to PI held by Signifi have signed a confidentiality agreement.
3. A process to receive, investigate and resolve questions or complaints from individuals, substitute decision makers and the public.
4. A program to monitor and audit access to records of PI to detect privacy breaches.
5. Investigation of privacy breaches and recommendations for corrective action to avoid similar breaches in the future.
6. Conducting, or overseeing the development of Privacy Impact Assessments for Signifi systems.
7. Development and publication of a Privacy Notice for stakeholders and the public.

The Ten Principles of PIPEDA Summarized

The ten Principles of PIPEDA that form the basis of this Privacy Policy are as follows:

1. Accountability: organizations are accountable for the personal information they collect, use, retain and disclose in the course of their commercial activities, including, but not limited to, the appointment of a Chief Privacy Officer;
2. Identifying Purposes: organizations are to explain the purposes for which the information is being used at the time of collection and can only be used for those purposes.
3. Consent: organizations must obtain an Individual’s express or implied consent when they collect, use, or disclose the individual’s personal information.
4. Limiting Collection: the collection of personal information must be limited to only the amount and type that is reasonably necessary for the identified purposes.
5. Limiting Use, Disclosure and Retention: personal information must be used for only the identified purposes and must not be disclosed to third parties unless the Individual consents to the alternative use or disclosure.
6. Accuracy: organizations are required to keep personal information in active files accurate and up to date.
7. Safeguards: organizations are to use physical, organizational, and technological safeguards to protect personal information from unauthorized access or disclosure.
8. Openness: organizations must inform their clients and train their employees about their privacy policies and procedures.
9. Individual Access: an individual has a right to access personal information held by an organization and to challenge its accuracy if need be; and
10. Provide Recourse: organizations are to inform clients and employees of how to bring a request for access, or complaint, to the Chief Privacy Officer, and respond promptly to a request or complaint by the individual.

Definitions

"Personal information" means any information about an identifiable individual. It includes, without limitation, information relating to identity, nationality, age, gender, address, telephone number, e-mail address, Social Insurance Number, date of birth, marital status, education, employment health history, assets, liabilities, payment records, credit records, loan records, income and information relating to financial transactions as well as certain personal opinions or views of an Individual.

"Business information" means business name, business address, business telephone number, name(s) of owner(s), officer(s) and director(s), job titles, business registration numbers (GST, RST, source deductions), financial status. Although business information is not subject to PIPEDA, confidentiality of business information will be treated with the same security measures by Signifi staff, members and Board members, as is required for individual personal information under PIPEDA.

"Client" means the business that is applying for or has been approved for a contractual relationship with Signifi Inc, (including sole proprietorships and individuals carrying on business in a partnership);

"Individual" means the client’s owner(s) or shareholders, co-signors, and/or any guarantor associated with a client.

"Member" means a person who volunteers on a Signifi committee, but who is not a current or active board member, or chair of the committee.

"Database" means the list of names, addresses and telephone numbers of clients and individuals held by Signifi in the forms of, but not limited to, computer files, paper files, and files on computer hard-drives.

"File" means the information collected in the course of processing an application, as well as information collected/updated to maintain /service the account.

"Express consent" means the individual signs the application, or other forms containing personal information, authorizing Signifi to collect, use, and disclose the individual's personal information for the purposes set out in the application and/or forms.  
  
"Implied Consent" means the organization may assume that the individual consents to the information being used, retained and disclosed for the original purposes, unless notified by the individual.

"Third Party" means a person or company that provides services to Signifi in support of the programs, benefits, and other services offered by Signifi Inc.

Collection of Personal Information:

It depends on the purpose for collection and the product or service involved. Below are some examples of when we may collect Personal Information:

* When you provide your Personal Information, during the inquiry, activation or purchase process for a product or service.
* When we provide service to our customers, including technical support or during the warranty, repair claims and service process.
* Automatically, when you use our products or services, or visit one of our websites (such as through the use of cookies or similar technologies), call into a call center.

Use of Personal Information

We use your Personal Information to provide you with our products or services.

We may also use your Personal Information to:

* Establish and maintain responsible commercial relations with you and to provide ongoing service.
* Try to understand the needs and preferences of our customers and determine your eligibility for products and services.
* Recommend products and services to meet your needs.
* Develop, enhance, market or provide products and services.
* Manage and develop business operations; or
* Meet our legal and regulatory requirements.
* Where necessary, we will request your further consent before using your Personal Information for any new purpose(s) beyond those described above.

Disclosure of Personal Information

We may disclose some of your Personal Information in a variety of circumstances, such as when we have your express or implied consent.

We may also disclose your Personal Information:

* To a person acting as your agent (such as a legal representative or authorized user) if we are reasonably satisfied that the person is authorized to receive your Personal Information.
* To our suppliers and authorized agents who assist with activities such as service installation or network maintenance, subject to strict security safeguards.
* To third-party collection agencies for the purpose of collecting amounts owed to us which are past due; to third parties, such as credit reporting agencies or anyone you have had a payment relationship with, to assess creditworthiness or assist with the collection of amounts owed to us which are past due and delivery organizations to ship you products and/or services you have ordered;
* To a government institution or another organization if reasonably necessary to establish your identity or to investigate the contravention of a law or an agreement or to prevent fraud.
* To an appropriate public authority in an emergency situation where there is imminent danger to life or property.
* As you have otherwise given us, or a third-party (like a financial institution, government agency, social media or other on-line site) your consent to do so; or
* As otherwise allowed or required by law. Where necessary, we will request your further consent before disclosing your Personal Information for any new purpose(s) beyond those described above.

Consent

An individual’s express, written consent will be obtained before or at the time of collecting personal information. The purposes for the collection, use or disclosure of the personal information will be provided to the individual at the time of seeking his or her consent. Once consent is obtained from the individual to use his or her information for those purposes, Signifi has the individual's implied consent to collect or receive any supplementary information that is necessary to fulfil the same purposes. Express consent will also be obtained if, or when, a new use is identified.

Limiting Collection

Personal information will be used for only those purposes to which the individual has consented with the following exceptions, as permitted under PIPEDA:

Signifi will use personal information without the individual's consent, where:

* The organization has reasonable grounds to believe the information could be useful when investigating a contravention of a federal, provincial or foreign law and the information is used for that investigation.
* An emergency exists that threatens an individual’s life, health, or security.
* The information is for statistical study or research.
* The information is publicly available.
* The use is clearly in the individual’s interest, and consent is not available in a timely way.
* Knowledge and consent would compromise the availability or accuracy of the information, and
* Collection is required to investigate a breach of an agreement.

Accuracy

Signifi endeavors to ensure that any personal information provided by the individual in his or her active file(s) is accurate, current and complete as is necessary to fulfill the purposes for which the information has been collected, used, retained and disclosed. Individuals are requested to notify Signifi of any change in personal or business information.

**Retention of Personal Information**  
Personal information will be retained in client files as long as the file is active and for such periods of time as may be prescribed by applicable laws and regulations.

Safeguards

Signifi will apply appropriate physical, administrative and technical safeguards to protect PI against loss or theft, or from unauthorized access, disclosure, copying, use, disposal or modification. Refer to Signifi Information Security Policy for more information.

Employees and members of Signifi committee(s) and/or Board of Directors are required to sign a confidentiality agreement binding them to maintaining the confidentiality of all personal information to which they have access.

Physical Safeguards: Active files are stored in locked filing cabinets when not in use. Access to work areas where active files may be in use is restricted to Signifi employees only and authorized third parties.

All inactive files or personal information no longer required are shredded prior to disposal to prevent inadvertent disclosure to unauthorized persons.

Technological Safeguards: Personal information contained in Signifi computers and electronic databases are password protected and encrypted in accordance with Signifi’s Information Security Policy. Access to any of the Signifi’s computers also is password protected. Signifi’s Internet router or server has firewall protection sufficient to protect personal and confidential business information against virus attacks and "sniffer" software arising from Internet activity. Personal information is not transferred to volunteer committee members, the Board of Directors, or third parties by e-mail or other electronic form.

Openness

Signifi will endeavor to make its privacy policies and procedures known to the individual via this Privacy Policy as well as the Signifi Privacy Statement. A version of this document will also be available on Signifi’s website.

Individual Access

An Individual who wishes to review or verify what personal information is held by Signifi Inc, or to whom the information has been disclosed (as permitted by the Act), may make the request for access, in writing, to Signifi 's Chief Privacy Officer. Upon verification of the individual's identity, the Chief Privacy Officer will respond within 60 days.

If the individual finds that the information held by Signifi is inaccurate or incomplete, upon the individual providing documentary evidence to verify the correct information, Signifi will make the required changes to the individual's active file(s) promptly.

Complaints/Recourse

If an individual has a concern about Signifi’s personal information handling practices, a complaint, in writing, may be directed to the Signifi’s Chief Privacy Officer.

Upon verification of the individual's identity, Signifi’s Chief Privacy Officer will act promptly to investigate the complaint and provide a written report of the investigation's findings to the individual.

Where Signifi’s Chief Privacy Officer makes a determination that the individual's complaint is well founded, the Chief Privacy Officer will take the necessary steps to correct the offending information handling practice and/or revise Signifi’s privacy policies and procedures.

Where Signifi’s Chief Privacy Officer determines that the individual's complaint is not well founded, the individual will be notified in writing. If the individual is dissatisfied with the finding and corresponding action taken by Signifi’s Chief Privacy Officer, the individual may bring a complaint to the Federal Privacy Commissioner at the address below:

Office of the Privacy Commissioner  
of Canada  
30, Victoria Street  
Gatineau, Quebec  
K1A 1H3

<https://www.priv.gc.ca/en/contact-the-opc/>

Toll-free: 1-800-282-1376  
Phone: (819) 994-5444  
TTY: (819) 994-6591

Policy Compliance

The Signifi team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to this policy must be approved by the CPO or CEO in advance.

Non-Compliance

Any violation of this Information Privacy Policy by an employee of Signifi is subject to disciplinary sanctions, as determined by Signifi Inc, up to and including dismissal.

Any violation of this Information Privacy Policy by a supplier, vendor or contactor or their respective employees and agents, is subject to remedies identified in the agreement or contract. Signifi may request the removal of a supplier, vendor or contractor employee who has violated this Information Privacy Policy.

Questions/Access Request/Complaint

Any questions regarding this or any other privacy policy of Signifi may be directed to the Chief Privacy Officer. Requests for access to information, or to make a complaint, are to be made in writing and sent to the Chief Privacy Officer at the address below:

Chief Privacy Officer – Razvan Anghelidi  
Email address: [privacy@signifi.com](mailto:privacy@signifi.com) ([ranghelidi@signifi.com](mailto:ranghelidi@signifi.com))   
Contact Number: 905-602-7707 x8164  
Signifi Solutions Inc   
1705 Tech Ave Unit 3, Mississauga, ON, L4W 0A2, Canada

**Amendment to Signifi’s Privacy Policy**

This Signifi’s Privacy Policy is in effect since 2016/01/29. The Privacy policy was approved by the Board of Directors & the CPO. This policy is subject to amendment in response to developments in the privacy legislation. The Chief Privacy Officer will review annually and revise the Privacy Policy as required by changes in privacy law. Notification of any changes in the Privacy Policy will be posted on Signifi’s website, as well as in Signifi’s Privacy Statement.

Data Controller Responsibilities

This section applies to clients that are hosted in the Signifi Canadian or European data center.

The client company is the Data Controller (“the custodian”).

Signifi is the Data Processor.

**Data Custodian Responsibilities**

1. The data controller is the principal party for data collection responsibilities.
2. The controller responsibilities include:
   1. collecting consent
   2. storing of the data (except where outsourced to a processor)
   3. managing consent-revoking
   4. enabling the right to access
3. Have the ability to demonstrate compliance with the principles relating to the processing of personal data. These principles are based on the use of personal data in the following list:
   1. lawfulness
   2. fairness
   3. transparency
   4. data minimization
   5. accuracy
   6. storage limitation and integrity
   7. confidentiality
4. Will maintain all records relating to a data breaches and act upon appropriate disclosure requirements

**Data Processor Responsibilities**

1. Upon receipt of any request related to personal data the Custodian will request of the Processor the removal of the revoked data from the Processor’s servers. Processor will act upon this request and provide confirmation of task completion
2. Secure data following industry standard encryption practises
3. Host the solution with stability and uptime targets set out in contracted Service Level Agreements
4. Provide backup and disaster recovery capabilities as set in the contract and SLA
5. Regular security testing
6. Ensure that the personal data that they process are kept confidential
7. Only process data in accordance with the Controller's instructions
8. Keep records of data processing activities aligned to pre-defined agreements
9. Ensure security of any personal data being processed
10. Involve decision-makers if a data breach occurs and report to the Controller within reasonable time limits
11. Assign an officer to oversee security of the data being processed
12. Lawfully transfer data as directed by the Custodian in a manner that ensure protection of the data being transferred
13. Not use the data for any purpose, including mining the data, that is not specifically instructed by the Controller

Enforcement

All instances of non-compliance will be reviewed by the department director. The department director, with the assistance of the Human Resources department has the authority to impose disciplinary actions, up to and including termination of employment or contractual agreement.

Update

This policy and all supporting documentation will be reviewed and updated annually or upon material changes to Signifi business rules, technology processes, organizational goals, or information security objectives to ensure its continuing suitability, adequacy, and effectiveness.

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| VERSION | DATE | SUMMARY OF CHANGE | CHANGED BY |
| 1.0 | 2016-01-29 | First version | Razvan Anghelidi |
| 2.0 | 2019-12-09 | Update format and content | Darace Rose |
| 2.01 | 2019-12-17 | Formatting | Razvan Anghelidi |
| 2.02 | 2020-02-18 | GDPR section added | George Plytas, Razvan Anghelidi |
| 2.03 | 2020-12-02 | Annual review | Razvan Anghelidi |
| 2.04 | 2021-03-15 | Minor edits | Razvan Anghelidi |
| 2.05 | 2021-12-12 | Annual review | Hadeel Alzuhairi |