



INTERNATIONAL FINANCIAL
DATA SERVICES

IFDS Canada Privacy Policy

International Financial Data Services (Canada) Ltd. ("IFDS") is committed to personal privacy and to the protection of personal information. For this reason, we have prepared this Privacy Policy pursuant to the *Personal Information Protection and Electronic Documents Act* and other applicable privacy legislation (collectively "Privacy Law").

IFDS provides market-leading transfer agency technology and services to the Canadian and global marketplace. This Privacy Policy summarizes, for the benefit of our employees, clients, our clients' distributors, as well as for individuals, the principles we, at IFDS, apply to the handling of personal information in our Canadian operations. All IFDS employees must adhere to these principles and to our personal information handling guidelines.

"Personal information" means information that identifies an individual, but does not include the type of information that would be found on a business card or through publicly available information such as the phone book. If the information cannot be directly associated with an individual, it does not fall within the statutory definition of "personal information".

This Privacy Policy is reviewed periodically and may be modified from time to time, as required, if there is a change to applicable laws, regulations and standards. The most up-to-date version can be obtained at our website at www.ifdsgroup.com or by contacting us at the address set out below in the section called "Contacting the Chief Privacy Officer".

All IFDS employees are mandated to complete an annual Privacy training program. This is done through our PACE Partner tool and is closely monitored for completion.

1. Collection, Use and Disclosure of Personal Information Relating to Clients

As a provider of transfer agency technology and services, IFDS does not directly collect, nor does it use, personal information from or about individuals for its own independent purposes. Rather, we receive personal information from our clients or their distributors for processing purposes. We operate under the direction of our clients and on the understanding that appropriate consents have been obtained, either expressly or implied, for the collection, use and disclosure of personal information. IFDS uses the personal information we receive solely to provide services to our clients in accordance with our contractual obligations and for no other purposes. Our staff is required, as a condition of employment, to limit access to and use of personal information to the extent necessary for the performance of their specific employment duties.

We do not use or disclose personal information for any marketing purposes.

2. Collection, Use and Disclosure of Personal Information Relating to Employees

We collect the personal information of our employees for recruiting and hiring purposes and in order that we can check references and properly administer payroll and benefit plans. Our human resources department collects the following employee information: name, address, telephone numbers, work and business information, banking information, social insurance number, driver's license number, dependent particulars, among other information. This information is collected and used for payroll and benefit plans setup, administration, payment and tax

remittance, to process any benefit or other claims, such as WSIB or medical related claims, and to comply with applicable employment legislation.

In addition, images, movements, actions, or other identifiable information about our employees may be captured by video equipment monitoring the common areas at offices and buildings under our management that an employee may visit as part of their duties.

Consent to use the information supplied by prospective employees is provided by means of the completion of an application for employment and/or acceptance of an offer of employment.

3. Collection or Disclosure w/o Knowledge or Consent

We may collect, use or disclose personal information without an individual's knowledge or consent in the following limited circumstances:

1. When the collection, use or disclosure of personal information is permitted or required by law;
2. In an emergency that threatens an individual's life, health or personal security;
3. Where we believe the individual would consent if asked and it is impractical to obtain consent (e.g. information obtained by a relative about an absent employee);
4. When we require legal advice;
5. To protect ourselves from fraud;
6. To investigate the breach of an agreement or a contravention of law.

4. Accountability

The following concepts are at the foundation of IFDS' approach to privacy protection as it relates to our clients, contractors and employees:

- IFDS will collect, use or disclose personal information only for authorized purposes.
- IFDS will comply with Privacy Law.
- IFDS will preserve the confidentiality, accuracy and security of personal information.
- These principles will guide us in the collection, use, retention and disclosure of personal information.
- IFDS' Privacy Policy will be applied with diligence and care to all our undertakings.
- Each employee is responsible for compliance with this policy in relation to the personal information under his/her control. In addition, IFDS has appointed a Chief Privacy Officer to assume overall responsibility for compliance with this policy and Privacy Law.
- Personal information will only be used for the purposes identified and access to personal information will be restricted to those who need to have access to it.

5. Service Providers

IFDS may retain an affiliated company or an independent third party ("authorized service provider") to perform, on our behalf, certain functions in support of the services we provide. Such functions could include, for example, application development, support, testing or transaction processing. Accordingly, in certain instances these

affiliates or third parties may be provided with access to personal information to the extent that it is necessary in the performance of those functions.

IFDS obligates its authorized service providers to use and take steps to protect personal information in accordance with the requirements of this Privacy Policy.

Some authorized service providers may be located in the United States of America or another foreign country other than Canada, and in those cases personal information may be subject to the laws of the jurisdiction in which it is situate. Written information about our policies and practices with respect to authorized service providers outside Canada, and answers to questions about such service providers, may be obtained by contacting us at the address set out below in the section called "*Contacting the Chief Privacy Officer*".

6. Security of Personal Information

As a processor of information on behalf of our clients, one of our most important privacy obligations is to take appropriate precautions to hold secure the information we receive. To that end, we apply security safeguards to our computing infrastructure and data in all forms. We maintain security policies, procedures and controls to protect the personal information we receive against loss or theft. We have safeguards in place to prevent unauthorized access, disclosure, copying, use and modification. We work with our clients to apply, to the extent that it is commercially and technologically feasible, the security standards required by our clients for the information we receive from them and which pertains to their business. Such safeguards and controls include, but are not limited to, the following:

1. Data security access control
2. Physical site access control
3. Network security
4. Virus protection
5. Intrusion detection
6. Remote use access control
7. Logical access control

We test and update, as appropriate, our safeguards and controls on a routine basis.

7. Retention and Access to Personal Information

IFDS retains personal information for the purposes described in this Privacy Policy and in accordance with our legal and contractual obligations to our clients. Personal information is stored at our offices in Canada or at the offices of an authorized service provider as required and defined under "*Service Providers*" above. Personal information is securely stored or disposed of in accordance with the instructions we receive from our clients.

Individuals have the right to access their personal information held by an organization and to challenge an organization about its personal information practices. However, as a provider of transfer agency technology and related services, IFDS does not respond directly to requests from individuals to access personal information or to complaints from individuals about the personal information practices of our clients. Any such requests and inquiries are referred back to our clients. This procedure is necessary to ensure that the authenticity of the request and the identity of the requester can be established by an individual's firm and/or the distributor, as applicable,

and that IFDS can receive specific instructions before personal information is released by IFDS on the individual's behalf.

8. Limiting Collection and Use

Personal information is collected only for the purposes set out herein and not indiscriminately. If we require information for any purpose not specified herein, the owner of the information will be notified of the new purpose and, subject to their consent, that new purpose will become an identified purpose. IFDS will only collect personal information by fair, lawful means and a responsible staff member will explain why the information is needed.

9. Limiting Disclosure and Retention

We will only disclose personal information as permitted by law. We do not sell or transfer any personal information outside of IFDS other than where explicit reference is made and approval obtained at the time the personal information is provided, or where passing that information to third parties is necessary to provide the information or service requested. Where we disclose personal information to a third party, we obligate that third party to use and take steps to protect personal information in a manner consistent with the provisions of this Privacy Policy.

IFDS has guidelines and procedures in place for the retention and destruction of personal information, taking into account legal requirements and restrictions. Personal information that has been used to make a decision about an individual will be kept for a reasonable time period so as to permit access to the information by the individual following the decision having been made. Information that does not have a specific purpose, or that no longer fulfils its intended purpose, will be destroyed in a secure manner.

10. Accuracy of Personal Information

We will strive to keep personal information as accurate, complete and up to date as necessary, taking into account its use and the interests of the individual. Personal information will only be updated when necessary to fulfill the purposes specified. We rely on individuals to disclose all material information to us and to inform us of any changes required. With proof of entitlement, a request to correct information in our possession may be made by contacting the Chief Privacy Officer at the address set out below in the section called "*Contacting the Chief Privacy Officer*"

Because the right to access information is not absolute, IFDS may decline access to information that we have under our control for reasons such as:

- the information subject to a legal privilege; or
- the information would reveal personal information about a third party.

Often all the individual has to do is ask, but it is possible we may request that the reason be stated in writing. If we cannot give access to the information requested, we will tell the person within 30 days, explaining as best we can why we cannot give access to the information. We will only refuse access as authorized by law, and in any event will provide the individual with a written explanation for refusing the request.

11. Challenging Compliance

To make a formal complaint about our privacy practices, or for more general inquiries, requests may be made in writing to our Chief Privacy Officer at 30 Adelaide Street East, Suite 1, Toronto, Ontario, M5C 3G9, Canada. The Chief Privacy Officer will acknowledge receipt of the complaint, ensure that it is investigated promptly and provide a formal decision and explanation in writing.

12. Contacting the Chief Privacy Officer

IFDS has appointed a Chief Privacy Officer to be responsible for its personal information practices and standards. Organizations, clients or individuals with questions or concerns about our personal information practices, or individuals who require assistance in making a request to access their personal information through one of our clients, can contact our Chief Privacy Officer. The Chief Privacy Officer's address is 30 Adelaide Street East, Suite 1, Toronto, Ontario, M5C 3G9, Canada.

Information Classification: **Public**

Creation Date: **November 15, 2007**

Last Reviewed: **November 22, 2019**

Changes: Significant changes by Legal Counsel on November 22, 2019

Version: **1.10**

Approved: **November 23, 2019 by Dennis Gregoris**

Approved: **December 11, 2019 by the Privacy Committee**

Policy Owner: **Dennis Gregoris, VP, Compliance & Chief Privacy Officer**