



EFFECTIVE FEBRUARY 27, 2018

Australia Privacy Policy Statement



Table of Contents

Purpose of the Policy	3
Personal information that OPTrust may collect	3
Purposes for which OPTrust may collect, use and disclose personal information	4
Third parties to whom OPTrust may disclose personal information	5
How personal information is held and protected by OPTrust	5
Accessing personal information held by OPTrust	5
Correcting personal information held by OPTrust	6
Privacy complaints and disputes	6
Contacting OPTrust about Privacy	7
Changes to this Policy & Statement	7
Further notes with respect to this policy	7
Amendment	8

Purpose of the Policy

OPSEU Pension Plan Trust Fund (“OPTrust”) is committed to maintaining the privacy and security of the personal information it collects and holds. Its organizational Privacy Policy applies directly to all staff. OPTrust’s office in Australia (“OPTrust AUS”) is also bound by the Australian *Privacy Act 1988* (Cth) (“*Privacy Act*”), which regulates the way in which the organization collects, holds, uses and discloses personal information in that country. OPTrust will manage personal information consistently with the requirements under the *Privacy Act*.

This Australia Privacy Policy and Statement (the “Policy”) is OPTrust’s:

- privacy policy for the purposes of the *Privacy Act* and provides information about how OPTrust manages personal information it collects about any individuals; and,
- privacy notification for the purposes of the *Privacy Act* and provides information on certain matters relevant to individuals whose personal information OPTrust may collect, hold, use and disclose from time to time.

This Policy applies to any of the individuals OPTrust may deal with, including but not limited to officers or employees of companies OPTrust is conducting due diligence on during a sales process, service providers or individuals that apply for, or gain, a role with OPTrust.

Personal information that OPTrust may collect

The type of personal information that OPTrust may collect and hold, and where that information comes from, will vary depending on the circumstances in which OPTrust is dealing with an individual.

This information may include:

- personal details such as an individual’s name, date of birth, residential and business addresses, telephone numbers (for example, where a person is an officer or director of a firm which is in a business relationship with OPTrust, a work electronic mail address or work telephone number);
- government identifiers such as a tax file number, ABN, Medicare card number, driver’s licence number or passport number (for example, to verify an identity if an individual applies for a position with OPTrust). OPTrust AUS does collect ABNs for payroll purposes (e.g. to withhold income tax and pay it to the tax office). Copies of identification may also be retained from staff for booking travel and accommodations;
- sensitive information, including place of birth or nationality, membership of a professional or trade association, criminal record check information and health

information (for example, if a person is a staff member, collection may include medical certificates and health related information associated with leave applications, workers' compensation matters, injury incidents and rehabilitation or other information used when booking travel arrangements);

- other details relating to a relationship and/or dealings with OPTrust (for example, if a person has applied for a position with OPTrust, pre-employment history, income, results of aptitude and other tests, contact and emergency details, pension and health insurance details).

Personal information is often collected by OPTrust directly from an individual. However, in some circumstances OPTrust may collect personal information from third parties. For example, where as part of assessing business acquisition opportunities, where we are provided personal information as part of our due diligence processes. OPTrust may also need to obtain personal information from a third party to verify information an individual has provided or to enable OPTrust to locate or communicate with that person.

Purposes for which OPTrust may collect, use and disclose personal information

OPTrust will collect, use or disclose an individual's personal information as is reasonably necessary for its business purposes and as permitted by law. Such purposes may include:

- recruitment and employment purposes;
- due diligence on directors, officers and senior management in relation to assessing business acquisition or investment opportunities;
- engaging service providers, contractors or suppliers relating to the operation of its business;
- dealing with complaints;
- meeting legal and regulatory requirements.

Various Australian laws may expressly require OPTrust to collect personal information or OPTrust may need to do so in order to be able to comply with other obligations under those laws. Such laws include the *Personal Property Securities Act* and State and Territory property and security interests laws (for example, to register and search for security interests) or the *Taxation Administration Act*, the *Income Tax Assessment Act* and other taxation laws (for example, to comply with obligations relating to employment or with information requests issued by the Commissioner of Taxation).

Third parties to whom OPTrust may disclose personal information

OPTrust may disclose personal information for the purposes listed above or as otherwise permitted by the *Privacy Act* to third parties that include the following:

- related companies, commercial partners and affiliates;
- service providers, information providers, advisers or agents;
- government and regulatory agencies, bodies and authorities;
- third parties authorized to act on behalf of OPTrust or that are otherwise connected (such as an accountant, legal representative, employer or referee);
- other persons that OPTrust needs to deal with in connection with engagement of staff (such as next-of-kin, training or medical providers); and
- other persons and entities as permitted under the *Privacy Act*.

Some of the recipients to whom OPTrust discloses personal information may be based overseas. In this instance it would include Canada, the OPTrust home office. Information that OPTrust sends in most cases would be to and from its offices and is primarily employee personal information required to maintain the employer-employee working relationship, administering the pension plan and employee benefits, etc.

How personal information is held and protected by OPTrust

OPTrust may hold your personal information in physical form or in electronic form on computer systems located in Australia or overseas. OPTrust stores your personal information in a secure manner and protects it from loss, theft, unauthorized access, disclosure, copying, use, modification or destruction of information through appropriate physical, administrative and technical security measures. OPTrust also implements internal policies and procedures intended to ensure that only personnel that require personal information to discharge their functions will access it.

As required by the *Privacy Act*, OPTrust will take reasonable steps to ensure that any personal information collected that is no longer required for a permitted purpose will be destroyed or permanently de-identified.

Accessing personal information held by OPTrust

You have a right to request access to the personal information that OPTrust holds about you, subject to certain exemptions under the *Privacy Act*. These are listed in the OPTrust Internal Privacy Policy.

Access requests may be made in writing or by telephone. See 'Contacting OPTrust about Privacy' below. OPTrust will normally respond to your request within 10 business days.

In the event that we refuse you access to your personal information, we will provide you with an explanation for that refusal. These reasons may include:

- where providing access will provide a serious threat to the life or health of any individual or pose an unreasonable impact on the privacy of other individuals;
- the request for access is frivolous or vexatious;
- the information relates to legal proceedings between us and you;
- the information would reveal our commercially-sensitive decision-making process; or
- we are prevented by law from disclosing the information or providing access.

Correcting personal information held by OPTrust

OPTrust takes all reasonable steps to ensure that the personal information it collects, uses or discloses is accurate, complete, up-to-date and relevant to the products or services provided to you or the nature of the relationship with you. If you believe that this is not the case in relation to any personal information OPTrust holds about you, you have the right to request that OPTrust correct your personal information. If you would like to request correction of your personal information please see "Contacting OPTrust about Privacy" below.

Privacy complaints and disputes

If you believe your personal information has not been treated consistently with the *Privacy Act*, please contact OPTrust – see "Contact OPTrust about Privacy" below.

OPTrust will investigate your privacy complaint and respond to you as soon as practicable. Where OPTrust finds that your complaint is justified, it will resolve the complaint. Where it disagrees with your complaint OPTrust will provide you with its reasons.

If you are unhappy with the handling of your complaint you also have the right to complain to the Office of the Australian Information Commissioner (visit www.oaic.gov.au for more information).

Contacting OPTrust about Privacy

If you wish to contact OPTrust about the privacy-related matters described above or find out more information about OPTrust's privacy practices, please use the contact details below:

Maurice Marnika

Data Protection Officer (Privacy Compliance & Risk Officer)

1 416 681-3612

Toll Free: 1 800 906-7738

mmarnika@optrust.com

Changes to this Policy & Statement

OPTrust may make changes to this document from time to time for any reason including, but not limited to, the introduction of new legislation. Any changes will be updated regularly through the OPTrust website.

The OPTrust office in Australia may retain personal information records about its staff including, home address, bank account details, superannuation account details and details of all personal investment holdings per our investment compliance policy. OPTrust retains personal information only as long as necessary to fulfill the purposes for which it was collected and in accordance with the OPTrust employee information retention schedule, unless personal information is required by law to be retained for a longer period of time. Normally payroll records are retained for a ten-year period. Some information may be shared with third party providers where such services are deemed as necessary.

OPTrust recognizes that there may be occasions when an individual may wish to deal with OPTrust by not identifying themselves or using a pseudonym. Where practical, this is acceptable to OPTrust.

Further notes with respect to this policy

- A copy of this document is available online on the OPTrust external website as well as the OPTrust Intranet.
- This document should be given to an individual at or before the time OPTrust collects personal information about the individual or, if that is not practicable, as soon as practicable after collection – for example, before OPTrust collects personal information from a prospective employee. However, if OPTrust is collecting business contact information about an individual only (for example, an officer's contact

details) it would be sufficient to refer the individual to the OPTrust Privacy Policy and Statement online.

- OPTrust will be required to take such steps as are reasonable in the circumstances to give a person a copy in whichever form they request (for example, in hard copy via mail).
- Any inquiries directed through the AUS office about this privacy policy should be forwarded to the Privacy Officer.

Amendment

The MDGC is responsible for amending the Policy. Amendments to the Policy shall be presented for discussion at the Operating Committee (the "OC") by the MDGC (or a delegate). The President & Chief Executive Officer (the "CEO"), shall approve the final version of the Policy (as amended based on the discussion at the OC, if applicable) and may dispense with the requirement that the Policy be presented to the OC at his or her discretion.

Amendments to the Policy which are of a technical/ administrative nature (e.g. changes for conforming purposes) may be approved by the CEO without discussion at the OC.

All amendments to the Policy shall be take effect on the date it is presented to the OC (or on the date it is approved by the CEO if not presented to the OC), unless another date is specified in the amendment.

Approved effective February 27, 2018



Hugh O'Reilly
President & Chief Executive Officer
OPTrust



OPSEU Pension Trust

Fiducie du régime de
retraite du SEFPO

1 Adelaide Street East, Suite 1200
Toronto, Ontario M5C 3A7

Telephone: 416 681-6161
Toll-free: 1 800 906-7738

optrust.com