

OMERS Administration Corporation Privacy Statement

COMPLIANCE & ETHICS



Kim Beatty
privacy@omers.com



Effective
January 24, 2019

OUR COMMITMENT TO YOUR PRIVACY

At OMERS Administration Corporation, we are committed to preserving the privacy of your personal data. This Privacy Statement elaborates on our commitment and helps provide transparency into our operations as they relate to your personal data.

As we evolve, the way in which we collect, use and disclose personal data may change. When this happens, we will update our Privacy Statement to reflect the changes and take steps to bring any material updates to your attention. You can review our updated Privacy Statement at any time by visiting our website, <http://www.omers.com>, or by requesting a copy from our Privacy Officer.

This Privacy Statement applies to the collection, use and disclosure of personal data within OMERS Administration Corporation (“OAC”), other than to the personal data of OAC’s employees, prospective employees or contractors, which is governed by OMERS Employee Privacy Statement.

What is personal data?

Personal data – often referred to as “personal information”, “personally identifiable information” or “PII” – is any information relating to an identified or identifiable person. An identifiable person is one who can be identified directly or indirectly from the information, taking into account any other information that OAC holds or could gain access to (including from public sources).

Personal data that we collect includes your name, contact information, and demographic information. It may also include “special categories” of personal data, which are of a more sensitive nature, including trade union membership and, indirectly, sexual orientation when you provide us information about your spouse. Other information of a more sensitive nature that we may collect include your national identifier (e.g., SIN) for tax reporting purposes and your health information for administration of disability benefits.

How is my privacy promoted?

Under the guidance of our Privacy Officer, OAC monitors and promotes compliance with privacy laws in jurisdictions where we operate, and with internal policies and procedures.

We have established processes for identifying potential privacy breaches and providing appropriate notification of any breaches that may cause real risk of significant harm to an individual or that may result in a risk to the rights or freedoms of



Underlying our commitment to privacy is the protection of personal data – information relating to an identified or identifiable person



Because your privacy is important to us, we carefully monitor its collection, use and disclosure.

an individual. This notification helps maintain accountability to the owners of personal data in our possession and control and allows them to mitigate risk. Where required by law, we will provide such notification without undue delay to affected individuals and/or any relevant supervisory authorities, but not later than within 72 hours of the discovery of the breach.

Why is personal data collected and what is it used for?

Knowing you helps us understand your needs, allows us to communicate effectively, and provide you with the services you want. Reasons we collect and use your personal data include the following purposes (the “identified purposes”):

- generally administering the OMERS Pension Plans;
- facilitating business transactions, including evaluating, effecting, monitoring and managing investments;
- establishing and maintaining member and stakeholder relationships;
- paying pensions and other benefits to members, spouses, survivors and others;
- providing you with the services you have requested or that you may be interested in;
- communicating with stakeholders, including employers;
- researching, developing, managing, protecting and improving our services, including conducting surveys that provide us with feedback on our service standards;
- tracking website usage, transaction history and patterns, for the purposes of market research and/or providing tailored messages;
- investigating specific transactions or patterns of transactions to detect unauthorized or illegal activities;
- maintaining appropriate records;
- evaluating, establishing and maintaining commercial relationships and fulfilling contractual obligations;
- monitoring and strategic oversight of our portfolio companies;
- facilitating safety and security;
- performing functions required or authorized by law, including meeting our statutory objects; and
- for any other purpose to which you consent.

Data collection and use practices may vary from jurisdiction to jurisdiction. For more details on how personal data is collected or used in your jurisdiction contact our Privacy Officer.

Is consent needed for collection, use and disclosure of my personal data?

While we strive to be transparent in our collection, use and disclosure of personal data, consent will not always be directly obtained.

However, we will only collect and use your personal data as reasonably necessary for the identified purposes, and only do so where there is a lawful basis. Sometimes this will be on the basis of consent. At other times it will be on the basis of a contractual obligation, legal obligation, our legitimate interests or vital interests, but in each case only to the extent necessary to fulfill that obligation or interest.



We collect, use and disclose personal data to serve you better and to fulfill our obligations to you and under the law.



The type of personal data we collect about you and the reason for the collection will depend on how you interact with us.



Whenever we collect, use and disclose your personal data, there is a lawful basis for doing so.

Where we do obtain your consent, subject to legal requirements, it can be withdrawn for OAC's collection, use or disclosure of your personal data by notifying our Privacy Officer in writing. If you withdraw your consent, this does not affect the lawfulness of any processing that we carried out prior to that withdrawal. Once we have received notification that you have withdrawn your consent, we will no longer process your personal data for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

We have set out below further information on our collection, use and disclosure of personal data.

Information You Provide To Us:

Our use of information you provide to us may include sharing it with our affiliates and service providers (for example, financial institutions and payment providers, actuaries, consultants, auditors, legal advisors, etc.)

If you provide us, our service providers, or our agents with personal data about another person, you represent that you have all necessary authority and/or have obtained all necessary consents from that individual to enable us to collect, use and disclose that personal data.

Pension Plan Administration:

When you enroll in the OMERS Pension Plans, we necessarily have to collect and use your personal information for their administration, and may share your personal information with others for this purpose.

As an example, if we are trying to locate you due to out-of-date contact information, we may share your name, date of birth, last known address and other out-of-date contact information with third-parties who provide locator services. When dealing with government entities (such as the Canada Revenue Agency) we may also share your SIN, which they will use in order to identify you.

We may also share information with other pension plan administrators to facilitate transfer of assets and to determine eligibility for transfer.



We collection, use and disclose your personal information in the course of pension plan administration.

Disclosure of Information to Employers for Other Purposes

The OMERS Pension Plans form part of your overall employment relationship with your employer. Unlike most private sector pension plans, employers who participate in the OMERS Pension Plans do not always have information about member pension accruals, and benefit entitlements that they may require for workforce and succession planning purposes, and for the purpose of other employment related benefit plans such as long term disability plans and insurance plans. As such, in addition to sharing information for the purposes of pension plan administration, we may share information about a member's hire date, enrolment date, total accrued service, unreduced early retirement date, and pension amounts after retirement (including disability pensions), solely for workforce and succession planning purposes and for the purposes of administering other employer benefit programs in which you are enrolled. Members who prefer that this information not be shared may send a written "opt out" request to our Privacy Officer.

Website:

Use of our website is subject to our policies and procedures.

Through our website, we may place a text file called a "cookie" in the browser directory of your computer's hard drive. A cookie is a small piece of information that a website can store on a web browser and later retrieve. The cookie cannot be read by any website other than the one that set up the cookie. Most browsers can be set to

reject all cookies. If you choose to modify your browser in this manner, some pages of our website may not function optimally and you may not be able to use all features of our website in the future.

Our website often provides links to websites that are operated by third-parties not under our control. This Privacy Statement does not describe the privacy policies of any third-party websites or their privacy practices. OAC is not responsible for how such third-parties collect, use or disclose your personal data, so it is important to familiarize yourself with their privacy policies before providing them with your personal data.

Secondary Marketing:

From time to time we may send you material that we believe may be of interest to you. Examples of such information include offers from our portfolio companies, our stakeholders, and charitable causes. We will not disclose your personal information to these parties without your consent.

Video Surveillance:

For safety and security reasons, we may use video surveillance technologies at our properties to monitor the public areas of those properties as well as internal meeting rooms.



For safety and security purposes, we use video surveillance on our properties.

We may disclose video surveillance footage to law enforcement or other government agencies where we believe such disclosure is: (i) permitted or required by law; (ii) necessary to protect our properties, visitors, customers or employees; or (iii) reasonable in connection with a law enforcement investigation.

Business Transactions:

We strive to limit collection, use and disclosure of personal data in the course of transactions, and do not exchange client lists as a matter of course. However, where reasonably necessary for business transactions, we may collect personal data from, or disclose personal data to third-parties. This may include information for background checks (including criminal and credit checks), or for proposed or actual purchase, sale (including a liquidation, realization, foreclosure or repossession), lease, merger, amalgamation or any other type of acquisition, disposal, transfer, conveyance, financing or investment.



We strive to limit collection, use and disclosure of personal data in the course of transactions.

Regulated Disclosures:

Where permitted or required by the law, we may disclose your personal data to government agencies in accordance with their statutory authority.

Where is my personal data stored and how long is it retained?

Usually your personal data is stored in the jurisdiction in which it was collected. However, OAC or our service providers and agents may store or access your personal data outside of the jurisdiction in which it has previously been collected, used or disclosed. For example, personal data collected in Ontario may be transferred outside of Ontario and/or Canada. Similarly, personal data collected within the European Economic Area (“EEA”) or the UK may be transferred to, and stored at, a destination within or outside of that area. When such transfer takes place, it may also be processed by staff operating outside of the jurisdiction who work for us or for one of our service providers.



Your personal data may be stored in, transferred to, and accessed from, a variety of jurisdictions.

When this transfer takes place, personal data may be subject to the laws of those other jurisdictions, and in certain circumstances, the courts, law enforcement agencies, regulatory agencies or security authorities in those other jurisdictions may be entitled to access your personal data. However, we will always ensure that your

personal data is adequately protected and transferred in compliance with applicable privacy laws. Further information is available on request from our Privacy Officer.

We retain personal data for only as long as it is needed to fulfill the identified purposes or as may be required to comply with applicable laws. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorized use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.



We keep your personal data only as long as it is needed.

In some circumstances we may anonymize your personal data so that it can no longer be associated with you, in which case we may use such data without further notice to you.

How is my personal data kept safe?

Whether in electronic or paper-based format, we implement appropriate technical and organizational measures to ensure an appropriate level of security, keeping in mind the nature, scope, context and purpose of processing, cost, and the potential risk to you. We use industry standard technology and efforts to safeguard your personal data from loss, theft and unauthorized access, use or disclosure. These include secure servers and firewalls. Physical access to those areas where information is gathered, processed or stored is restricted to authorized employees who require the information to perform a specific function. Appropriate controls are in place over computer systems and data processing procedures and these controls are reviewed on an ongoing basis to ensure compliance with our security and privacy requirements.



We use a variety of mechanisms – including technical and organizational measures – to help keep your personal data secure.

We require our service providers and agents to protect personal data processed on our behalf.

How can I access, correct, transfer or delete my personal data?

We try to ensure that the personal data we collect about you is accurate, complete and up-to-date. However, we rely on you to provide accurate information in the first instance, and to notify us when there is a change in your personal data. In certain circumstances we may verify personal data, or obtain additional personal data through third-parties.



We rely on you to help us keep our records accurate, but may occasionally seek external verification.

In some jurisdictions, you have a right to access, correct, transfer or delete your personal data in our possession or control, or to object to our processing of your personal data. This may be done by writing or emailing our Privacy Officer.

Who can I contact with questions or concerns?

If you have any comments or questions about our Privacy Statement, or if you believe that we have not complied with our Privacy Statement, please contact our Privacy Officer as follows:



Our Privacy Officer is ready to respond to your questions and concerns.

Kim Beatty,
Privacy Officer
900-100 Adelaide Street West
Toronto ON M5H 0E2
e-mail: privacy@omers.com

You may also have the right to make a complaint to the relevant supervisory authority for data protection and privacy issues. For more information, contact our Privacy Officer.