Employee
Privacy Statement

PRIVACY

Kim Beatty

Effective
October 11, 2022

OVERALL PRINCIPLES

OMERS is committed to preserving the privacy of the personal data of our Employees, prospective Employees and Contractors. 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 intranet or requesting a copy from OMERS Privacy Officer.

This Privacy Statement applies to the collection, use and disclosure of the personal data of Employees, prospective Employees and Contractors of OMERS. For the purpose of this statement OMERS refers to the OMERS group company with which you are employed (in the case of current Employees) or to which you are applying for a role (in the case of prospective Employees).

What is personal data?

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

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 OMERS holds or could gain access to (including from public sources).

It may also include “special categories” of personal data, which are of a more sensitive nature. These special categories include personal data about ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of identification, or data concerning health or concerning a person’s sex life or sexual orientation.

How is my privacy promoted?

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

Under the guidance of OMERS Privacy Officer, we monitor and promote 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 an individual. Where required by law, we will provide such notification without undue delay to affected individuals and/or any relevant supervisory authorities.

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

We collect, use, and disclose personal data to manage employment, post-employment, and contractual relationships.

In general, we collect Employee, prospective Employee and Contractor personal data to establish, manage and administer employment, post-employment, and contractual relationships. Reasons we collect your personal information include the following purposes (the "identified purposes"):

- determining eligibility for initial and ongoing employment, including the verification of references and qualifications as part of a background check;
- administering all human resources policies and programs throughout employment, including managing talent, diversity and inclusion initiatives, employee engagement, learning and development, health and safety, evaluation of performance, compensation, and benefits;
- managing and promoting OMERS businesses, including for regulatory reporting or compliance purposes;
- acquiring and transferring businesses;
- protecting OMERS against and investigating error, fraud, and misconduct;
- drawing insights from our Employee data, in order to improve performance and culture;
- facilitating safety and security;
- performing functions required or authorized by law;
- for any other purpose to which you consent.

We may combine personal data that we have about you and apply advanced analytics such as content and sentiment analysis to that data to derive insights that will help us to improve our services.

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 OMERS Privacy Officer.

What is the legal basis for collection, use and disclosure of personal data?

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

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 your consent. In the European Economic Area ("EEA") and the UK we generally rely upon our legitimate business interests to process your personal data (such as our collection of personal data to confirm your suitability for a job or to administer the employment relationship). However, at other times the legal basis will be a contractual obligation to you (such as our use of your bank account details to pay your salary) or a legal obligation (such as when we are obliged to provide your personal data to legal or regulatory authorities).

When processing special categories of personal data the legal basis may be consent (such as our diversity and inclusion initiatives), our legitimate interest (such as short term illness management), that the processing is necessary for the exercise or fulfilment of rights and obligations arising from employment and social security and social protection law (such as when you leave employment for reasons

of ill health or disability or for purposes of health care or occupational medicine), to protect your vital interests (such as an emergency situation where we need to contact you), or that the processing is necessary for purposes of health care or occupational medicine for the assessment of your work ability as an employee (such as when we process data to ascertain your fitness for work).

In each case we will only collect, use, or disclose your personal data to the extent necessary for the purposes mentioned above.

Where we do obtain your consent, subject to legal requirements, it can be withdrawn by notifying OMERS 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 who assist us with our business operations. Some of the categories of service providers we use include: information technology providers (such as cloud hosting services and software services), professional services providers (such as auditors, lawyers and consultants), specialized service providers (such as training services and background check providers), and benefit and financial service providers (such as banks and insurance companies). If our affiliates and service providers handle personal information on our behalf, they are required to protect that personal information and to use it only to provide the services we request. Further information on the recipients of your personal data is available from OMERS Privacy Officer.

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.

Background Checks:

We will only undertake background checks where reasonably necessary in the circumstances and permitted by law.

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.

Video Surveillance:

For safety and security reasons, we may use video surveillance technologies at our offices and 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.

Electronic Monitoring:

We monitor OMERS facilities, networks, and assets (including mobile devices) in order to detect, prevent and investigate error, fraud, or misconduct as well as threats to the security and operation of our IT systems This may include by using data loss prevention software. As such, while we permit your use of OMERS facilities, networks and assets for limited personal purposes, any personal information involved may be collected and/or accessed as part of our monitoring.

We monitor your use of OMERS facilities, networks, and assets.

We may make employment decisions based on your use of OMERS facilities, networks, and assets and/or disclose information to law enforcement and other authorities in circumstances that we view as appropriate.

See Appendix 1 for further details on our electronic monitoring practices.

Regulated Disclosures:

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

Intranet(s):

Use of our intranet(s) is subject to our policies and procedures.

Through our intranet(s) including our careers portal, 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 intranet(s) sometimes provides links to or embed content from 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. OMERS 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.

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

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

OMERS and our service providers may transfer, store, or access your personal data outside of the jurisdiction in which it has been collected, used, or disclosed. Transfers of your personal data will be made in compliance with applicable privacy laws and where there are suitable safeguards in place. For example, personal data collected in EEA or UK may be transferred to Canada on the basis of the European

Commission's adequacy decision relating to Canada or under an agreement based on standard contractual clauses that have been approved by the European Commission for the transfer of data from the EEA (a copy of which is available through OMERS Privacy Officer). When a 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. Further information on appropriate safeguards in place in respect of transfers of your personal data is available on request from OMERS Privacy Officer.

We retain personal data in accordance with our document retention guidelines and 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 your 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. Employee personal data is generally retained for a period of seven years from the date that the employment relationship has terminated. The personal data of prospective employees who were not hired will generally be retained for a period of two years from the date that the job competition closed. In some jurisdictions the legal requirements for retention may be for longer or shorter periods and OMERS endeavors to ensure that local practices align with local requirements.

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?

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

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

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.

In some jurisdictions such as the EEA and the UK, 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 OMERS Privacy Officer.

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

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 this Privacy Statement, please contact OMERS Privacy Officer as follows:

Kim Beatty

OMERS Privacy Officer

900 – 100 Adelaide Street West

Toronto, ON M5H 0E2

e-mail: kbeatty@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 OMERS Privacy Officer.

Appendix 1- Electronic Monitoring

Tool	How	When	Purpose
Mobile Device Management	Monitoring mobile phones for information security, including IP location of access for unusual access location or if reported lost or stolen.	Continuous	Information Security; Investigations
Endpoint Detection and Response (EDR)	Monitoring the use of workstations (programs run, files read and written, etc.) and comparing it against a baseline to detect abnormalities and potential unauthorized use.	Continuous	Network Security; Information Security; Investigations
Access card	Monitoring physical access in and out of company premises.	When used	Physical Security; Investigations; Space planning
Virtual private network (VPN) Monitoring	Monitoring the network logins and the IP location of devices used by remote workers to access corporate network.	When used	Information Security; Investigations
System Login Monitoring	Tracking login/logout of systems.	Intermittent (when logging in and out)	System Security; Investigations
Information Technology Usage Activity Monitoring	Tracking file upload or download on company devices; Tracking attempts to install non-approved applications on mobile devices.	Continuous (when used)	Network and System Security; Investigations
Email and Chat Monitoring	Monitoring in-coming and out-going emails and chat messages to detect and prevent malicious activity or external attacks such as phishing and spam and to detect inappropriate behavior.	Continuous/ intermittent	User Protection; Monitoring acceptable use of company resources; Information Security; Investigations
Customer Service Technology Monitoring	Recording of interactions on customer service platforms.	Continuous	Quality Assurance; Investigations
Web Monitoring	Monitoring web browsing activities and monitoring requests to detect and protect against various known & unknown Phishing, Malware, Ransomware attacks.	Continuous	User protection; Monitoring acceptable use of company resources; Investigations