

## Employee Privacy Notice

AltaGas Ltd. and its subsidiaries and affiliates (the "Company") are committed to protecting the privacy and security of your personal information while you are an employee and after your employment ends for any reason. The Company manages the collection, use, and disclosure of personal information in accordance with applicable data protection and privacy laws in the jurisdictions in which we have employees, and subject to the terms and conditions of any applicable collective bargaining agreement. This Privacy Notice applies to all employees and former employees, independent contractors, and job applicants of the Company. It also applies to all personal information that we collect, use, and disclose regarding your emergency contacts and beneficiaries and by providing such information you confirm that you have permission to provide such information to us.

### Categories of Personal Information We Collect

We collect information that may be "personal information" according to applicable law. Subject to applicable law, this information may include information that identifies you, your household, your device, or that is reasonably capable of being connected with or linked to you, your household, or your device ("Personal Information"). The Company only collects Personal Information that is necessary for operating its business, which may include the following:

- Identifiers
  - First and last name
  - Email address
  - Mailing address
  - Phone number
  - Birth date
  - Place of birth
  - Social Security Number / Social Insurance Number
  - Driver's license Number
  - Passport and other government identification numbers
  - Employee photos for identification badges and system profiles
  - Emergency contact information including relationship to employee
  - Dependent and beneficiary information
- Characteristics of Protected Classifications
  - information regarding minority, veteran, age, gender, religious, and disability status (which may vary from jurisdiction to jurisdiction)
- Commercial Information
  - Bank routing and deposit information
- Biometric Information
  - Not collected, however biometric information may be used by employees to log-in to Company equipment and to access secured Company locations
- Internet or Other Electronic Network Activity Information
  - Cookies
  - Domain name
  - Browser type
  - Operating system
  - Usage data
- Geolocation Data
  - Information that tells us from where you access our website if you are applying for a job or working remotely
  - Information that tells us where Company work vehicles are located
- Professional or Employment-Related Information
  - Résumé/CV
  - Job title, job status, department, and job code
  - Work authorization status and related documents not otherwise listed
  - Withholding tax information

- Dependent and beneficiary information
- Pay information such as pay rate, lump sum payments, and payroll deduction information
- Direct deposit information
- 401(k) loan information (for US employees)
- Leave of absence information
- Other information necessary to administer benefits
- Performance management information such as employment status (full-time or part-time, regular or temporary), work schedule, job assignments, hours worked, business travel information, expatriate and secondment assignments, accomplishments and awards, training and development information, performance evaluation information, discipline and counselling information, and employment termination information
- HIPAA approved medical record set (for US employees)
- Health and safety information such as health condition, job restrictions, drug testing information, workplace accident and illness information, and health insurance information
- Employment history
- Background check information
- Information relevant to securities law disclosures
- Non-public Education Information
  - Educational information relevant to hiring qualifications
- Inferences Drawn from Other Personal Information
  - Performance management information derived from other information above.

### Personal Employee Information

To the extent permitted by applicable privacy legislation, the Company may collect, use or disclose Personal Information of any potential, current or former employee without their consent for the purposes of establishing, managing or terminating the employment relationship, or managing the post-employment relationship. As required and necessary, the Company will provide you with notice that your Personal Information will be collected, used or disclosed, including the purposes for which such information will be collected, used or disclosed.

Your Personal Information may be collected, used, and disclosed for purposes including, but not limited to:

- in the case of an emergency;
- hiring, promotion and compensation;
- compliance with legal requirements and obligations;
- compliance with requirements of applicable professional governing bodies;
- provision and administration of health and welfare benefits and programs;
- human resources and payroll administration;
- professional development and performance management; and
- enforcement of the Company's policies and procedures.

### Categories of Sources of Personal Information

We generally collect information from the following sources:

- Directly from you. For example, when you provide information to us when applying for a job or using our employee on-boarding processes. We also collect information about dependents and beneficiaries directly from you.
- From third parties. For example, we collect certain identifiers and employment related information from recruiters and companies that we use to perform background checks. We also collect information from job candidates through our Workday enterprise resource planning software.

The Company will seek your consent to collect, use or disclose Personal Information, but may do so without your consent if doing so is authorized or required by law. The Company may imply consent in cases where you volunteer information for an obvious purpose.

You may withdraw your consent to the use and disclosure of Personal Information at any time unless the Personal Information is necessary to fulfill the Company's legal obligations. The withdrawal of your consent to the use and disclosure of Personal Information may mean that the Company will not be able to provide you with certain benefits, etc.

### How We Use Your Personal Information

- We use all of the above information to onboard new employees, comply with applicable laws, comply with government requests for information, meet our contractual obligations and to initiate or respond to legal claims.
- We use Identifiers, Internet or Other Electronic Network Activity Information, Geolocation Data, Professional or Employment-Related Information, and Inferences Drawn from Other Personal Information to perform human resource functions, manage your employment and administer benefits.
- We use Identifiers, account information, and Professional or Employment Related Information to administer payroll, reimbursements, and benefits and to provide work-related items such as payment cards and access cards.
- We use Characteristics of Protected Classifications to implement our diversity programs and to comply with applicable laws.
- We use Professional or Employment-Related Information such as health and safety Information to maintain a safe workplace, assess your working capacity, to establish, manage, or terminate the employment relationship or manage the post-employment relationship, administer health and Workers' Compensation insurance programs, and comply with applicable laws.
- We use Identifiers and Biometric Information to ensure that employees properly log-in to our equipment and ensure that only authorized employees have access to secured locations of the Company.
- We use Internet or Other Electronic Network Information to protect the Company, customer, and employee property, equipment, and confidential information; monitor employee performance; and enforce the Company's electronic communications acceptable use policies.

The Company protects Personal Information in a manner appropriate to the sensitivity of the information. The Company will make every reasonable effort to prevent loss, misuse, disclosure, copying, modification, disposal or destruction of Personal Information or any unauthorized access to Personal Information. Access to your Personal Information is limited to those individuals who require such Personal Information to carry out their responsibilities.

The Company will retain Personal Information only for as long as is reasonable to fulfil the purposes for which the information was collected or for legal or business purposes and will employ appropriate measures to render Personal Information non-identifying or destroy Personal Information, including shredding paper records and permanently deleting electronic records, once the information is no longer necessary

### *Prohibitions of the Use of Social Security Numbers (for US Employees Only)*

Applicable law, including the Michigan Social Security Number Privacy Act ("SSNPA") states that employers shall not intentionally do any of the following with the SSNs of their employees:

- Publicly display all or more than 4 sequential digits of the SSN;

- Use all or more than 4 sequential digits of the Social Security Number as the primary account number for an employee;
- Visibly print all or more than 4 sequential digits of the Social Security Number on any identification badge or card, membership card, or permit or license;
- Require an individual to use or transmit all or more than 4 sequential digits of his or her Social Security Number over the Internet or a computer system or network unless the connection is secure or the transmission is encrypted;
- Require an individual to use or transmit all or more than 4 sequential digits of his or her Social Security Number to gain access to an Internet website or a computer system or network unless the connection is secured, the transmission encrypted, or a password or other unique personal identification number or other authentication devices is also required to gain access to the Internet website or computer system or network;
- Include all or more than 4 sequential digits of the Social Security Number in any document or information mailed to the person.

The following are exceptions in which Social Security Numbers can be used:

- Disclosure to governmental agencies as required by law
- Applications and enrollment processes initiated by an individual
- Documents related to employee health insurance benefits
- As required by state or federal statute, court order, or pursuant to a legal discovery process

## How We Share Your Personal Information

We share Personal Information in each of the above categories as follows:

- All categories of Personal Information
  - We will share Personal Information in all the above categories if the Company is sold or we engage in a merger or other such transaction.
  - We will share Personal Information in all the above categories in connection with a law enforcement request that is compliant with applicable laws.
- Identifiers, Internet or Other Electronic Network Activity Information, Geolocation Data, and Professional or Employment-Related Information
  - We share this Personal Information to service providers who use such information only to provide services to us such as sending postal mail or email, processing job applications, administering benefits, recruiting, background checks, administering HR and payroll services and processing data.
  - We share some of this Personal Information with our security service providers to protect the Company's property, equipment, and people.
  - Workers' Compensation vendors will receive no more than name, address, date of birth, gender, income, age, marital status, and email addresses.

We also may disclose Personal Information in special cases. For example, when we believe that we must disclose information to identify, contact, investigate or bring legal action against someone who may be violating our Terms of Service, Master Service Agreement or applicable laws, policies and procedures including the Acceptable Use of Technology and Social Media Policy or Code of Business Ethics (as applicable), or may be causing injury to or interference with our rights or property, other website users or customers and their information, or anyone else who may be harmed by such activities. We may disclose access or monitor your Personal Information when we believe

in good faith that applicable law requires it and for administrative and other purposes that we deem necessary to maintain, service and improve our products and services and our information security.

The Company may, from time to time, transfer Personal Information to its affiliates located in another country, including between Canada and the United States. Such affiliates may receive, process, and handle Personal Information for the purposes described in this Privacy Notice and will provide a level of protection for Personal Information that is comparable to that provided by the Company. However, while the Company will take all appropriate measures to prevent the use or disclosure of Personal Information, other than as required for the purposes set out in this Privacy Notice, Personal Information processed and stored in a foreign jurisdiction may be accessible to foreign government agencies, including law enforcement and national security authorities.

Additionally, the Company may disclose Personal Information to other third-party service providers for the purposes of providing services or functions on behalf of the Company. Personal Information will not be disclosed to such third-party service providers except as described in this Privacy Notice, with your consent or as required or permitted by applicable law. The Company will endeavor to ensure that its contracts with third party service providers limit the retention, use and disclosure of Personal Information by the third-party service provider solely for the purpose of carrying out the contracted services and provide a level of protection for Personal Information that is comparable to that provided by the Company.

### **Violations of this Privacy Notice**

If you become aware of a material breach in Personal Information or confidential information, you should immediately report the incident to management. The Company has the responsibility to investigate the incident and take corrective action. Violations of this Privacy Notice should be reported immediately to management. Any employee found in violation of this Privacy Notice will be subject to disciplinary action including discharge for just cause. Violation may also result in criminal and civil liability. None of the statements included in this Privacy Notice are intended to limit or restrict any protected rights under the U.S. National Labor Relations Act or other applicable law.

### **Who Do I Contact for More Information?**

If you have any questions or concerns regarding this Privacy Notice or the collection of your personal information, please contact a member of the Compliance team.

You may access your Personal Information in the Company's custody or control, subject to certain exceptions. For example, applicable law may prohibit access to information that may contain Personal Information about another person or confidential business information. Access may also be refused if the information is subject to solicitor-client privilege. If refusing a request in whole or in part, the Company will provide the reasons for the refusal, as may be required by applicable law. In some cases where exceptions to access apply, the Company may withhold that information and provide the remainder of the information.

You may make a request for access to your Personal Information by writing to your Human Resources Business Partner. Sufficient information must be provided in the access request to allow the Company to identify the information you are seeking. You may also request information about the Company's use of your Personal Information and any disclosure of that information to persons outside the organization.

Additionally, you may request a correction if there is an error or omission in your Personal Information.

If you are not satisfied with a response or you have a complaint, you may contact the applicable Privacy Commissioner or regulator in your jurisdiction.