



PROTECTION OF PERSONAL INFORMATION POLICY

PURPOSE AND SCOPE

This Policy governs TransCanada's Use of Personal Information, and complies with federal, provincial, and state privacy and Personal Information protection statutes and regulations.

This Policy applies to all Personnel, Third-Party Suppliers and other individuals to whom TransCanada's Use of Personal Information applies.

The Policy works in conjunction with and does not replace, amend, or supplement any collective bargaining agreement a union has with TransCanada. It is not intended to restrict communications or action protected or required by any law.

TransCanada's Privacy Officer is accountable for this Policy. People may contact the Privacy Office for all matters related to TransCanada's Use of Personal Information.

DEFINITIONS

Contractors means Contract Workers, Independent Contractors, and Independent Consultants as defined in the Contingent Workforce Policy.

Good Faith Reporting means an open, honest, fair and reasonable report made without malice or ulterior motive.

Identifiable Individuals means, but is not limited to, individual Personnel, stakeholders, customers, and landowners in accordance with this Policy.

Identified Purposes means the reason(s) Personal Information is required by TransCanada to fulfill business needs or comply with applicable laws.

Personal Health Information (PHI) means all individually identifiable health and medical information held or transmitted by TransCanada or a third-party stakeholder. PHI includes people's past, present or future physical or mental health; any healthcare provided; past, present or future payment for the provision of healthcare to people; or people's accommodation requests for medical reasons.

Personal Information means any information TransCanada has collected that identifies or could identify people and is protected by law. Personal Information protected by law includes but is not limited to age, date of birth, gender, race, ethnicity, religious affiliation, disabilities, family details, marital status, salary,



benefits, social security numbers, social insurance numbers, national identification numbers, licenses, home addresses, personal phone numbers, personal email addresses, training records, employee numbers, employment history, resumes, photographs, opinions about other people (e.g., references, interview notes, performance appraisals), identifying remarks and other sensitive or private information. People's names, job titles, business addresses, business email addresses and business phone numbers are not protected by law.

Personnel means full-time and part-time employees and Contractors of TransCanada.

Privacy Breach means loss of, unauthorized access to, or unauthorized disclosure of Personal Information. Privacy Breaches occur when Personal Information is stolen, lost or inappropriately shared, either inadvertently or purposely.

Privacy Office means the TransCanada group designated to assist and support the duties and obligations of TransCanada's Privacy Officer.

Privacy Officer means the TransCanada employee designated to receive requests to access or amend Personal Information as well as complaints about Use of Personal Information, notifications about possible Personal Information breaches, and questions or concerns about TransCanada's Use of Personal Information. TransCanada's Privacy Officer may delegate various duties and functions to members of the Privacy Office as appropriate.

Third-Party Supplier means an external supplier providing materials or services under an agreement with TransCanada.

TransCanada or the Company means TransCanada Corporation and its wholly-owned subsidiaries and operated entities.

Use of Personal Information means Personal Information TransCanada collects, maintains, transmits, holds, stores, discloses, retains, destroys or otherwise uses while doing business.



POLICY

COLLECTION OF PERSONAL INFORMATION

Personal Information will be collected in accordance with applicable law.

TransCanada and, where applicable, Third-Party Suppliers must identify the reasons for collecting Personal Information prior to collection and obtain consent when required for Use of Personal Information.

The amount and type of Personal Information collected must be limited to what is needed to fulfill Identified Purposes.

Written Consent for PHI

Written consent must be obtained to collect, use or disclose PHI except in the event such consent is not required by law.

PHI consent forms must be written in plain language, describe PHI to be used or disclosed, identify whose PHI is being disclosed, identify which person or organization is receiving PHI, include the expiry date of consent, notify the person that they may in writing revoke consent to the PHI pertaining to them and contain any other relevant data.

USE AND DISCLOSURE OF PERSONAL INFORMATION

Use of Personal Information must be for Identified Purposes only. Exceptions may be made only with the person's consent or if authorized by law.

Personal Information about Identifiable Individuals must be disclosed only to those people with a reasonable need to see it.

If Personal Information was collected as part of a Canadian investigation of a breach of agreement or contravention of law, TransCanada will notify the Canadian Privacy Commissioner in writing. In the U.S. and Mexico, it will be managed according to federal and state law.

Use and Disclosure of PHI

PHI may be disclosed to Third-Party Suppliers for benefits administration and as authorized by law.

In the U.S., TransCanada is required to disclose PHI to the U.S. Department of Health and Human Services when undertaking a compliance investigation or review or enforcement action, regardless of the person's consent. People in the U.S. may



request TransCanada restrict use or disclosure of PHI. If TransCanada agrees to the request, the Company must comply with the agreed restrictions except for treating people in medical emergencies.

ACCESS TO PERSONAL INFORMATION

People may contact the Privacy Officer to request access to their Personal Information. Requests must be made in writing and be related to TransCanada's Use of Personal Information for Identified Purposes. For requests that originate other than from a TransCanada email address, or for any third-party requests, additional verification information will be required.

Please refer to the Acceptable Use Policy regarding Personal Information (e.g., personal contacts, pictures) stored on TransCanada devices.

Response to Requests for Access to Personal Information

TransCanada responds to written requests for access to Personal Information within thirty calendar days or as required by law. A fee for costs incurred may be charged for complex requests, however people will be informed of fees in advance.

People will be informed of the Use of their Personal Information and be given access to such Personal Information as required by law. Requested Personal Information will be provided in the form in which it is kept. Where Personal Information has been collected by a Third-Party Supplier on TransCanada's behalf, the Company will direct people to such Third-Party Supplier regarding requests for access.

TransCanada will be as specific as possible when describing Third-Party Suppliers to whom it has disclosed Personal Information.

People may either view original records or request copies as permitted or required by law. To preserve the integrity of records and ensure documents are not removed from TransCanada, people viewing original records will be supervised by designated Personnel.

Limitations to Access

In some situations, TransCanada may be unable to provide access to all Personal Information it holds about people.

TransCanada will inform people in writing of the Company's reasons for such inability, if applicable, and any recourse people may have to challenge TransCanada's decision.



MAINTENANCE OF PERSONAL INFORMATION

Personal Information must be kept as accurate, complete and up-to-date as needed for Identified Purposes.

Amendment of Personal Information

People may update or amend incorrect Personal Information by making a written request to the Privacy Officer.

Security and Retention of Personal Information

Personal Information will be retained only while needed for Identified Purposes and will be disposed of in a manner appropriate for the sensitivity of the Personal Information. Please refer to the Records Classification System and Retention Schedule for more information.

Personal Information must always be protected by security safeguards appropriate to the sensitivity of information. Please refer to the Information Security Policy for additional information.

PERSONAL INFORMATION AND ANTI-SPAM LEGISLATION

Written consent for Use of Personal Information does not constitute consent to communicate electronically with people. Please refer to the Communications Policy for information about Canada's Anti-Spam Legislation (CASL). CASL applies to any electronic messages received within Canada.

PRIVACY IMPACT ASSESSMENTS

TransCanada conducts Privacy Impact Assessments (PIAs) to evaluate solutions related to Use of Personal Information. PIAs enable TransCanada to comply with legal obligations, to identify and minimize privacy-related risks and to manage Personal Information effectively. Solutions include (1) development or acquisition of new systems or applications or (2) updates or modifications to existing systems or applications. These solutions may be TransCanada-based, supplier-based or cloud-based.

PIAs are initiated via standard processes established with Information Services and Supply Chain. Internal requests for PIAs outside these processes must be submitted to the Privacy Officer.



COMPLIANCE AND PRIVACY BREACHES

The Privacy Officer will report Privacy Breaches to government authorities and notify affected people of a breach, in accordance with applicable legal requirements.

Should a Privacy Breach happen at TransCanada, Personnel must stop the Privacy Breach if possible. Real or suspected breaches must be reported immediately to both the Information Services Service Desk and the Privacy Officer.

The Privacy Officer manages Privacy Breach investigations with involvement of the Law Department. People must cooperate in an honest and forthright manner with Privacy Breach investigations and resolutions.

Inquiries or complaints about compliance with this Policy may be submitted in writing to the Privacy Officer, or alternatively, in Canada to the Privacy Commissioner of Canada or relevant provincial authority; in the U.S. to the U.S. Department of Health and Human Services (for PHI); and in Mexico to the Federal Institute of Access to Information and Data Protection.

COMPLIANCE

Personnel must comply with all aspects of this Policy and support others in doing so. Personnel are responsible for promptly reporting suspected or actual violation of this Policy, applicable law, or any other concern, through available channels so that it can be appropriately investigated, addressed and handled. Personnel who fail to comply, or knowingly permit Personnel under their supervision to not comply, may be subject to appropriate corrective disciplinary action in accordance with the Company's Policies and process. Please refer to the TransCanada Corporate Policies website for more information.

NON-RETALIATION

We support and encourage Personnel to report suspected incidents of non-compliance with applicable laws, regulations, policies and authorizations, as well as hazards, potential hazards, incidents involving health and safety or the environment, and near hits. We take every report seriously, investigate each report to identify facts, and effects improvements to our practices and procedures when warranted. All Personnel making reports in good faith will be protected. Good Faith Reporting is intended to remove protection for Personnel making intentionally false or malicious reports, or who seek to exempt their own negligence or willful misconduct by the act of making



a report. We ensure immunity from disciplinary action or retaliation for Personnel for the Good Faith Reporting of such concerns. Reports can be made to management, a compliance coordinator, or anonymously to the Ethics Help-Line.

REFERENCES AND LINKS

- [Policy Questions and Comments](#)
- Acceptable Use Policy
- Code of Business Ethics Policy
- Communications Policy
- Corporate Security Policy
- Information Management Policy
- Information Security Policy
- Privacy Officer
- Records Classification System and Retention Schedule