DATA COMMUNICATIONS MANAGEMENT CORP.

Information Security and Privacy Policy Statement

Why do we have a privacy policy?

Like companies across Canada, DATA Communications Management Corp. (DATA) must abide by the Personal Information Protection and Electronic Documents Act (PIPEDA). PIPEDA regulates the collection, use and disclosure of personal information. This federal law, along with "substantially similar" laws in some provinces, stipulates that no collection, use or disclosure of personal information can be done without consent.

Personal information is defined as information about an identifiable individual, but does not include the name, title, business address or telephone number of an employee of an organization.

Customer information

We are responsible for a customer's or third party's personal information that has been transferred or received with their consent in the course of doing business with them. We are responsible for ensuringhat information is secure, used correctly, and disposed of properly.

We do not collect or use personal information for its own purposes. As a third-party service provider, we use customers' personal information for the sole purpose of producing and and distributing communication. It is the customer's sole responsibility to ensure the personal information they've provided is accurate and that they have appropriate consent to use it. By supplying this information to DATA, the customer authorizes that we may use it to complete a specific task on their behalf; however, they maintain full liability regarding information accuracy and individual consent.

Our collection and use of information is governed by PIPEDA's 10 principles of privacy:

1. Accountability

DATA is responsible for personal information in its control. As a result, the company has designated an individual, Genevieve Goldie Pagnotta, as Chief Privacy Officer (CPO). As CPO, she is accountable for DATA’s compliance with the 10 principles.

2. Identifying purposes

The purpose of the information and the way it is to be used must be clearly identified before DATA receives it. There are specific protocols for its transmission and handling, including project ID and individual access codes, which must be communicated to all relevant internal and external parties.

3. Consent

When a customer requires DATA to collect third-party personal data on their behalf, it is the customer’s responsibility to ensure the information collected is limited to the requirements of the corresponding project.

4. *Limiting collection*

Collection of personal information is limited to purposes related to and identified by DATA. Information must be collected in line with appropriate contractual arrangements, and by fair and lawful means, from sources such as credit bureaus or other relevant third parties.

5. *Limiting use, disclosure and retention*

Personal information is not to be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual, or as required or permitted by privacy laws. Personal information will be retained only as long as necessary for the fulfillment of those purposes or as required by law.

6. *Accuracy*

DATA keeps information as accurate, complete, and current as possible, updating it when necessary, or upon request.

7. *Safeguards*

DATA maintains appropriate physical and technological safeguards in all its facilities. File transfers containing personal information from outside sources must be encrypted and password-protected. Accepting unencrypted files is prohibited. Feel free to forward any concerns to your manager or directly to the CPO.

8. *Openness*

DATA maintains an open-door policy on all our privacy practices, internally and externally, in written and email form, to all our employees and business partners. DATA's privacy policy is available on our website at www.datacm.com.

9. *Individual access*

Other than prohibited by law, all information has been and continues to be accessible upon request, within a reasonable time period.

10. *Challenging compliance*

To address a concern regarding DATA's privacy compliance, please contact DATA's Chief Privacy Officer. DATA will respond to all complaints within 30 days. If it is justified, the company shall take appropriate measures to resolve it, including, if necessary, amending our privacy policy and related practices.

A downloadable version of our Privacy Policy is available in PDF format. If you have any questions or comments, or wish to file a complaint regarding our policy, please contact our Chief Privacy Officer:

Mr. Douglas Groff
Tel: (905) 791-3151
Fax: (905) 791-3277
Email: privacy@datacm.com