JUNE 2015

CYBERSECURITY BULLETIN

Borden Ladner Gervais

REGULATORY GUIDANCE FOR SAFEGUARDING PERSONAL INFORMATION

On June 10, 2015, the Office of the Privacy Commissioner of Canada issued *Interpretation Bulletin – Safeguards* to provide non-binding guidance for compliance with statutory obligations to safeguard personal information. The guidance provided by the *Interpretation Bulletin* is timely in light of the June 18, 2015 enactment of the *Digital Privacy Act*, which includes amendments (not yet in force) to the *Personal Information Protection and Electronic Documents Act* that will impose notice, reporting and record keeping obligations in connection with a data security breach that creates a real risk of significant harm to an individual.

STATUTORY SAFEGUARDING OBLIGATION

Canada's federal *Personal Information Protection and Electronic Documents Act* ("PIPEDA") regulates the collection, use and disclosure of personal information in the course of commercial activities by organizations in all provinces except British Columbia, Alberta and Québec (each of which have substantially similar provincial personal information protection laws) and by organizations that operate a "federal work, undertaking or business" or transfer personal information across provincial borders for consideration. PIPEDA requires compliance with a *Model Code for the Protection of Personal Information*, which includes Principle 7 – "Personal information shall be protected by security safeguards appropriate to the sensitivity of the information". The *Model Code* elaborates on that general principle as follows: (1) the required safeguards must protect personal information (regardless of the format in which the information is held) against loss or theft, as well as unauthorized access, disclosure, copying, use or modification; (2) the nature of the required safeguards will vary depending on the sensitivity of the information, the amount, distribution, and format of the information, and the method of storage; and (3) the safeguards should include physical measures, organizational measures and technological measures.

INTERPRETATION BULLETIN

The *Interpretation Bulletin* provides non-binding legal interpretations and guidance, derived from referenced court decisions and regulatory findings, for compliance with statutory obligations to safeguard personal information. Following is a summary of some of the guidance:

- **Policies, Practices and Procedures:** Organizations must put in place security safeguards that are commensurate with the level of sensitivity of the personal information involved. Safeguarding policies and practices must be diligently and consistently followed. One of the best safeguarding practices an organization can have is not to collect or retain more personal information than is necessary. Proper safeguarding of personal information includes diligent and accurate record-keeping practices that clearly document original authorizations and any irregular uses or disclosures of personal information.
- **Sensitive Information:** More sensitive information (e.g. payroll information, medical information, social insurance numbers, work performance information and some biometric data) requires a higher level of protection.
- **Employee Training:** Organizations must educate and train their employees to ensure that the organization's safeguarding procedures are implemented correctly.
- **Third Party Organizations:** Organizations that transfer personal information to third parties must ensure that the third parties have proper safeguards in place to protect the personal information.
- **Client Identification and Authorization:** Organizations must have safeguards in place and follow proper client-authentication procedures to guard against unauthorized third-party access to personal information. Organizations must be particularly vigilant when safeguarding personal information in situations involving family relationships, joint account holders, individuals living in the same household or having similar names.
- **Mail, E-Mail, and Fax:** When mailing or faxing personal information, organizations must have safeguards in place to confirm that only the personal information of the intended recipient is delivered and the proper destination address or fax number is used. When mailing personal information, organizations must ensure that no sensitive personal information is visible through the address window of the envelope, and envelopes containing personal information that are sealed by a machine must be double checked to ensure they have been properly sealed before being mailed out. Organizations must ensure fax cover sheets do not contain sensitive personal information. When e-mailing multiple recipients, organizations must ensure that individual recipients' e-mail addresses are not disclosed.

- **Technology:** Organizations that store personal information online must ensure that the information is adequately protected by passwords or encryption. Organizations that use portable electronic devices to store personal information must ensure that the devices are properly secured at all times. Devices that store personal information must be encrypted, password protected and backed up. Organizations that transfer sensitive personal information via the Internet must employ sufficient safeguards such as data encryption. Organizations must keep abreast of technological advances to ensure that their technological safeguards, including encryption standards, are up to date.
- **Storage:** Documents containing personal information must be stored in an appropriate location to prevent unauthorized access. Personal information, such as fingerprints and drivers' licence numbers, should be encrypted, stored in a locked cabinet and accessible only to a limited number of authorized personnel.
- **Responding to a Security Breach:** Organizations that have breached their privacy obligations should inform affected individuals without delay. In cases of suspected theft or fraud, an organization should inform police as soon as possible. Where safeguards have proven inadequate, organizations must take immediate steps to enhance safeguards through updated employee training, new or revised protocols and strengthened procedures.

COMMENT

The guidance provided by the *Interpretation Bulletin* is timely in light of the June 18, 2015 enactment of the *Digital Privacy Act*, which includes amendments (not yet in force) to PIPEDA that provide that if a "breach of security safeguards" (which is broadly defined in the *Act* to include a failure to establish security safeguards) for personal information under an organization's control creates a real risk of "significant harm" (which is broadly defined in the *Act* to include humiliation, damage to reputation and identity theft) to an individual, then the organization must report the breach to the Privacy Commissioner, give notice of the breach to each affected individual and to certain organizations and government institutions and keep and maintain prescribed records of the breach. Compliance with the guidance provided by the *Interpretation Bulletin*, including the recommended use of data encryption technology, may reduce the risk of a breach of security safeguards or the risk that significant harm will result from a data breach. ■

AUTHOR

Bradley J. Freedman
T 604.640.4129
bfreedman@blg.com

Borden Ladner Gervais

BORDEN LADNER GERVAIS LLP
LAWYERS | PATENT & TRADEMARK AGENTS

Calgary
Centennial Place, East Tower
1900, 520 – 3rd Ave S W, Calgary, AB, Canada T2P 0R3
T 403.232.9500 | F 403.266.1395

Montréal
1000 De La Gauchetière St W, Suite 900, Montréal, QC H3B 5H4
T 514.879.1212 | F 514.954.1905

Ottawa
World Exchange Plaza, 100 Queen St, Suite 1300
Ottawa, ON, Canada K1P 1J9
T 613.237.5160 | F 613.230.8842 (Legal)
F 613.787.3558 (IP) | ipinfo@blg.com (IP)

Toronto
Scotia Plaza, 40 King St W, Toronto, ON, Canada M5H 3Y4
T 416.367.6000 | F 416.367.6749

Vancouver
1200 Waterfront Centre, 200 Burrard St, P.O. Box 48600
Vancouver, BC, Canada V7X 1T2
T 604.687.5744 | F 604.687.1415

blg.com