SEPTEMBER 2018

PRIVACY BULLETIN

Borden Ladner Gervais

Preparing for Compliance with New Privacy Consent Guidelines

Commencing January 1, 2019, the Privacy Commissioner of Canada will begin enforcing *Guidelines for obtaining meaningful consent*, which impose requirements and provide recommendations for private sector organizations to obtain legally valid consent for the collection, use and disclosure of personal information. The Guidelines specify requirements for the form and content of privacy policies/notices and for clear and easily accessible privacy consent processes. Private sector organizations should review and revise (if necessary) their privacy policies/notices, privacy consent processes and personal information practices and procedures, so that they are able to demonstrate compliance with the Guidelines.

Fundamental Principles

Canadian private sector personal information protection statutes – the Canadian *Personal Information Protection and Electronic Documents Act* ("PIPEDA"), the Alberta *Personal Information Protection Act*, the British Columbia *Personal Information Protection Act*, and Québec's *An Act respecting the Protection of Personal Information in the Private Sector* – are based on internationally recognized *Fair Information Principles*. Three of those fundamental principles are openness, identified purposes and consent.

- **Openness:** An organization must be open about its personal information policies and practices, and must enable individuals to easily acquire understandable information about those policies and practices.
- **Identified Purposes:** An organization must identify the purposes for which it collects, uses and discloses personal information, and must disclose those purposes (orally or in writing), at or before the time the information is collected, to the individual from whom the information is collected.
- **Consent:** An individual's informed consent is required for the collection, use and disclosure of the individual's personal information, except in specified, limited circumstances in which consent is inappropriate.

PIPEDA further provides that an individual's consent is valid only if it is reasonable to expect that the individual understands the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting.

Privacy Policies and Related Notices

Many organizations use privacy policies and related notices as the primary means of obtaining informed consent to their personal information practices, and to fulfil obligations under the openness and identified purposes principles. Canadian privacy commissioners have previously issued guidance to help private sector organizations implement effective privacy policies. For example: *Ten Tips for a Better Online Privacy Policy and Improved Privacy Practice Transparency* (October 2013); *Interpretation Bulletin: Form of Consent* (March 2014); *Guidelines for Online Consent* and *Frequently Asked Questions for Online Consent* (May 2014); *Ten Tips for Communicating Privacy Practices to Your App's Users* (September 2014); and *Interpretation Bulletin: Openness* (August 2015).

Helpful guidance regarding privacy policies and related issues may also be found in privacy commissioner investigation reports, such as the *Report of Findings* and *Takeaways for all Organizations* relating to the Ashley Madison data breach investigation.

Guidelines for Obtaining Meaningful Consent

In May 2018, the Office of the Privacy Commissioner of Canada and the Offices of the Information and Privacy Commissioners of Alberta and British Columbia jointly issued *Guidelines for obtaining meaningful consent* (the "Guidelines") to provide practical, actionable guidance to help private sector organizations obtain legally valid consent to the collection, use and disclosure of personal information. The Guidelines criticize "the use of lengthy, legalistic privacy policies" that too often make individual control enabled by consent "nothing more than illusory", and explain that the requirements and best practices summarized in the Guidelines are intended to "breathe life" into the ways that consent is obtained.

Guiding Principles

The Guidelines identify seven principles for private sector organizations to follow to obtain meaningful consent.

- **Emphasize key elements:** For consent to be valid, an organization must provide individuals with readily accessible, comprehensive and understandable information about the organization's privacy practices. Information "buried in a privacy policy or terms of use serves no practical purpose" for most individuals. An organization must enable individuals to quickly review key information "right up front" as they are engaging with the organization. For this purpose, organizations must generally put additional emphasis on the following key elements: (1) details of the personal information being collected; (2) the third parties with whom personal information is shared; (3) the purposes for which personal information is collected, used or disclosed; and (4) any residual meaningful risk (more than a minimal or mere possibility) of harm (including reputational harm) and other consequences arising from the collection, use and disclosure of personal information.
- **Allow individuals to control the level and timing of detail:** An organization must provide individuals with information about the organization's privacy practices in manageable and easily accessible ways (e.g. by presenting information in layers), and individuals should be able to control how much detail they wish to obtain and when they obtain it (e.g. information should remain available for later access).
- **Provide individuals with clear options to say "yes" or "no":** An organization must provide individuals with clearly explained and easily accessible choices about consenting to the organization's collection, use or disclosure of personal information beyond what is necessary for the organization to provide requested products or services to the individual (unless an exception to the general consent requirement applies). Whether consent must be express/opt-in or implied/opt-out will depend on the circumstances.
- **Be innovative and creative:** Organizations should use innovative consent processes tailored to the specific circumstances, including: "just-in-time" privacy notices that appear when personal information is collected; interactive tools to aid in the presentation of privacy information; and customized mobile interfaces to address the small screen and timing challenges of providing privacy information on a mobile device.
- **Consider the consumer's perspective:** Organizations must implement consent processes that are user-friendly, easily accessible from all relevant devices (e.g. mobile devices, tablets, gaming devices and computers), understandable (e.g. clear explanations and suitable language) by all target audiences, and customized to the nature of the relevant product or service, so that relevant individuals can easily access and understand the organization's personal information practices.
- **Make consent a dynamic and ongoing process:** Organizations should consider consent to be an ongoing, dynamic and interactive process that does not end with the posting of a privacy policy. Organizations should use interactive or dynamic tools to anticipate and answer users' questions, and should provide individuals with periodic privacy reminders. Organizations must obtain relevant individuals' consent before implementing significant changes to privacy practices, including the use of information for new purposes or sharing information with new third parties. Organizations should periodically audit their personal information practices for compliance with relevant privacy policies.
- **Be accountable:** Organizations should be able to demonstrate that their consent processes are sufficiently understandable to result in valid consent from relevant target audiences. The steps an organization is required to take to demonstrate compliance will depend on the size of the organization and its personal information practices.

Related Issues

The Guidelines also provide guidance regarding issues related to consent.

- **Form of Consent:** Organizations must obtain individuals' personal information consents in an appropriate form – express consent or implied consent – depending on the particular circumstances. Consent should generally be express, but it can be implied in "strictly limited circumstances". An organization must generally obtain an individual's express consent if the information collected, used or disclosed is sensitive, or if the collection, use or disclosure of the information is outside the individual's reasonable expectations or creates a meaningful, residual risk of significant harm (including reputational harm) to the individual.
- **Consent and Children:** The ability of minor children to give meaningful personal information consent depends on their maturity and ability to understand the nature and consequences of their privacy choices. A parent or legal guardian may give personal information consent on behalf of a minor child who is not able to give valid consent. The Office of the Privacy Commissioner of Canada takes the position that, in all but exceptional circumstances, children under 13 years old are not able to give valid personal information consent, and instead consent must be obtained from their parents or guardians.
- **Appropriate Purposes:** The purposes for which an organization collects, uses and discloses personal information must be defined and limited to purposes that a reasonable person would consider appropriate. The limiting principle of appropriate purposes is discussed in *Guidance on inappropriate data practices: Interpretation and application of subsection 5(3)* (May 2018).

- **Withdrawal of Consent:** Individuals have the right to withdraw personal information consent, subject to legal or contractual restrictions, and organizations must respect consent withdrawals. An individual's withdrawal of consent may require the deletion of previously collected personal information.
- **Other Obligations:** Consent does not alleviate the need to comply with other privacy law obligations, including the fundamental principles of accountability, data minimization, and safeguards.

The Guidelines include a useful checklist that summarizes the guidance into "must do" measures required to satisfy legal requirements, and "should do" measures that reflect recommended best practices.

Comment

The Guidelines are generally consistent with previously issued guidance, but impose new requirements for the form and content of privacy policies/notices, and for providing individuals with clear and easily accessible choices for the collection, use or disclosure of their personal information beyond what is necessary for requested products and services. The Guidelines will likely be a key enforcement tool for the PIPEDA Compliance Directorate, which was established in 2018 to investigate PIPEDA complaints by individuals and complaints initiated by the Privacy Commissioner of Canada.

Compliance with the Guidelines will likely require many organizations to revise their privacy policies/notices and adjust some of their personal information practices and procedures. When engaged in that process, organizations should consider other important privacy law requirements (e.g. an appropriate, documented information security governance framework) and be mindful of PIPEDA's new personal information security breach obligations, which will come into force on November 1, 2018. For more information, see BLG bulletins: *Regulatory Enforcement Action Emphasizes Need for an Information Security Governance Framework* and *Canadian Personal Information Security Breach Obligations – Preparing for Compliance*. ■

Authors

Bradley J. Freedman
T 604.640.4129
bfreedman@blg.com

Katherine McNeill
T 604.640.4150
kmcneill@blg.com

BLG's Privacy/Data Protection Law Group and Cybersecurity Law Group help clients manage cyber risks, achieve legal compliance and respond to security incidents across Canada. More information is available at blg.com/privacy and blg.com/cybersecurity.

Key Contacts

Bradley J. Freedman	Vancouver	604.640.4129
Éloïse Gratton	Montréal	514.954.3106
Ira Nishisato	Toronto	416.367.6349
Robert J. C. Deane	Vancouver	604.640.4250

BORDEN LADNER GERVAIS LLP
LAWYERS | PATENT & TRADEMARK AGENTS
Borden Ladner Gervais LLP is an Ontario Limited Liability Partnership.

This document provides general information only, and does not constitute legal or other professional advice. Readers are encouraged to obtain legal advice from a competent professional regarding their particular circumstances. Copyright © 2018 Borden Ladner Gervais LLP.

BLG Vancouver
1200 Waterfront Centre, 200 Burrard St
Vancouver, BC, Canada V7X 1T2
T 604.687.5744 | F 604.687.1415
blg.com