ACCESS REQUESTS

Posted on July 5, 2015

Categories: Insights, Publications

Individuals are becoming increasingly attentive to the manner in which organizations handle their personal information, as well as the activities of public bodies that control a vast repository of data. As a result, access to information requests are common. Therefore, it is important for organizations and institutions to understand their obligations upon receipt of an access request, as well as the circumstances when access can be denied.**Private Sector**

Under the *Personal Information Protection and Electronic Documents Act* ("PIPEDA"), and substantially similar provincial legislation, individuals generally have the right to access their own personal information[1] (subject to certain exceptions described below). "Personal information" is broadly defined as "information about an identifiable individual,"[2] and can include information contained in documents (hard copy or electronic), as well as photographs, video and audio recordings, and biometric information. Personal information does not include information that is not about an individual, such as product information.

The right to access personal information includes the right to:

- Be informed of whether the organization holds information about the individual;
- An explanation of how personal information is being or has been used;
- A list of organizations to which the personal information has been (or may have been) disclosed;[3] and
- Access personal information in a form that is generally understandable and accommodates any sensory disabilities.

In addition, individuals have the right to challenge the accuracy and completeness of personal information held by the organization, and to have it amended if it is inaccurate or incomplete. Where appropriate, the amended information may need to be provided to any third party who received the original information.

Organizations typically must respond to access requests within certain time limits and at little or no cost to the individual.[4] They are also obligated to help individuals who require assistance with preparing an access request.[5]

Organizations are required to search all locations and files under their control for personal information (not just the most obvious sources containing such data). However, absent special circumstances, organizations are not

generally required to recover information that was deleted or overwritten prior to receiving an access request.

Provincial privacy legislation that is substantially similar to PIPEDA contains similar requirements related to providing access to personal information.

Exceptions

Although individuals generally have a broad right to access their own personal information, there are some limits on this right. For example, under PIPEDA, the organization cannot provide access to information if doing so would likely reveal personal information about a third party.[6] In addition, under PIPEDA, the organization is generally[7] not required to provide access to personal information if:[8]

- the information is protected by solicitor-client privilege;
- the information would reveal confidential commercial information;
- providing access could reasonably be expected to threaten the life or security of another individual;
- the information was collected without the individual's knowledge and consent for reasonable purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province;[9]or
- the information was generated in the course of a formal dispute resolution process.[10]

Similar exceptions exist under substantially similar provincial privacy legislation. However, in some of the situations outlined above, if the organization can sever the information that falls within the exempt category, then it must do so and provide the individual with access to any remaining personal information.

When access is denied, the individual must be informed in writing and provided with reasons as well as an explanation of any potential recourse under PIPEDA.

Best Practices

The OPC has published a "step-by-step guide of best practices" for responding to PIPEDA access requests, which can be found at: *https://www.priv.gc.ca/resource/fs-fi/02_05_d_54_ati_02_e.asp*. Similar principles would apply when responding to access requests under substantially similar provincial legislation, however, some of the provincial privacy commissioners have established their own guidelines which should also be taken into consideration.

Public Sector

The *Privacy Act* allows Canadian citizens, permanent residents and individuals located in Canada to access personal information about them that is held by federal government institutions.[11]In addition, the *Access to Information Act* ("AIA") allows certain persons to access records under the control of federal government

institutions.[12]However, like the private sector legislation described above, public sector legislation contains some limits upon access rights. For example, under the AIA, the government institution generally cannot release records containing:[13] (i) trade secrets; (ii) confidential financial, commercial, scientific or technical information belonging to a third party; (iii) personal information pursuant to the *Privacy Act*; or (iv) confidential information of other governments and government institutions.[14]

Each of the provinces has also enacted legislation that provides for a right of access to certain records held by provincial and/or municipal government institutions. For example, in Ontario, there is the *Freedom of Information and Protection of Privacy Act* as well as the *Municipal Freedom of Information and Protection of Privacy Act*.

Each statute governing access to information held by government institutions contains specific provisions respecting the information that is accessible, the process for making access requests, and exceptions to access rights. For more information on access requests under public-sector legislation, please contact your McMillan advisor who will connect you with a member of *McMillan's Privacy Group*.

Tips for Compliance

In order to satisfy statutory requirements related to access requests, organizations should have clear and straightforward procedures in place for responding to such requests. The need for such procedures has been stressed by the Office of the Privacy Commissioner of Canada in prior cases. As always, staff should be properly trained to follow such procedures and ensure that the organization complies with its legal obligations.

by Lyndsay Wasser

[1] Proof of identity may be required before providing access to personal information.

[2] PIPEDA s. 2.

[3] Some exceptions may apply if the information was disclosed in response to a subpoena, warrant or court order, or if it was disclosed to a government institution for purposes related to national security, national defence, deterrence of terrorism, law enforcement, or in relation to suspected money laundering. See PIPEDA s.9(2.1) to 9(2.4).

[4] PIPEDA, Schedule 1, Article 4.9.4

[5] PIPEDA s.8

[6] Unless the third party consents or the individual needs the information because a person's life, health or security is threatened

[7] Some exceptions exist, such as where the individual needs the information because a person's life, health or security is threatened.

[8] PIPEDA s. 9.

[9] Permitted under PIPEDA if it was reasonable to expect that collection with knowledge or consent would have compromised the availability or accuracy of the information.

[10] This list is not all-inclusive.

[11] As defined in the *Privacy Act*.

[12] As defined in the AIA.

[13] AIA ss. 13 to 20.

[14] This list is not all-inclusive.

A Cautionary Note

The foregoing provides only an overview and does not constitute legal advice. Readers are cautioned against making any decisions based on this material alone. Rather, specific legal advice should be obtained.