Tipsheet for Organizations: How to Gather and Manage Sensitive Information

This tipsheet helps organizations understand how to meet the requirements regarding gathering and managing sensitive information described in the TSM Equitable, Diverse and Inclusive Workplaces Protocol's Indicator 1 regarding Leadership and Strategy (Corporate Criteria) and Indicator 3 regarding Monitoring, Performance and Reporting.

Organizations often gather and manage sensitive information while developing and implementing strategies and action plans supporting equity, diversity and inclusion (EDI) in the workplace. Sensitive information includes data that requires protection, as the loss, misuse or modification of such data could result in harm to an organization, groups within the organization and/or individuals. Sensitive information could relate to talent pool, financial, health or socioeconomic data, including data related to EDI. This may include personal information related to identity, such as ethnicity, sexual orientation, gender identity, age, disability status, citizenship or immigration status, organizational information related to pay or employment equity, incident reporting and resolution or even highly sensitive information related to personal safety planning.

Mining companies that operate in Canada and collect and manage sensitive information are obligated to maintain data confidentiality and anonymity. Businesses are bound by privacy laws and regulations at the federal and provincial levels. At the federal level, the Personal Information Protection and Electronic Documents Act (PIPEDA) governs "how private-sector organizations collect, use, and disclose personal information."[1] Some provinces have privacy laws that are similar to PIPEDA, specifically for health, education and employment data.

Gathering Sensitive Information

1. Create a Data Management Policy

Before collecting sensitive information, ensure that corporate data collection and usage policies are in place, aligned with the appropriate regulatory frameworks and shared internally as well as with any information providers. Such policies address communication protocols, as well as information gathering and sharing, data storage and destruction practices. They identify the different methods of data collection that may be used (e.g., survey, interview, focus group, etc.) and appropriate measures to ensure sensitive information is gathered, managed, stored and destroyed appropriately. Sharing the policy with stakeholder groups – including employees – demonstrates transparency and compliance with the regulatory environment(s) in which the company operates. Data collection and storage tools used for personal and/or sensitive information should support compliance with the corporate data management policy.

1 Office of the Privacy Commissioner, *Summary of Privacy Laws.* Businesses that conduct commercial, for-profit activities are subject to PIPEDA, as are federally-regulated organizations in terms of employee data. PIPEDA does not apply to organizations that operate entirely within Alberta, British Columbia or Quebec.

2. Obtain Consent

Before providing any data, individuals are made aware of the risks associated with sharing their information to support understanding and ensure that informed decisions are made about any information shared, that is, informed consent. Similarly, an individual must be capable of understanding the associated risks to provide consent or have a legal guardian present to provide consent. When the information being gathered is sensitive, consent can be given by means of a clear verbal or written indication – usually the latter; providing or refusing consent via a simple 'yes or no' – that can be withdrawn at any time. To support awareness of risks, inform individuals of the following:

a) For what purpose is personal information being collected, used or disclosed?

Give individuals information about the purpose for collecting data, the aims that data collection and use intends to fulfil and if applicable, why and under what circumstances it will be shared or disclosed. Significantly, indicate whether the information will only be used in ways that protect the confidentiality and/or anonymity of individuals.

b) What personal information is being collected?

Inform individuals of the specific information that is being collected, the scope or restrictions of its intended use and whether participation in the data collection process is mandatory or voluntary. It is also an effective practice to provide options for responding to sensitive questions, offering respondents an opportunity to "Prefer not to say," for example.

c) Who will personal information be shared with?

Provide individuals with information about who will be working with the information shared and who will have access to it, including whether data will be shared with a third party, and if so, which one, to what end and how it will be managed.

d) Risk of harm and other consequences?

Ensure individuals are aware that although policies and tools are put into place to mitigate risks of harm, risks still exist. To the extent possible, identify and share any foreseeable risks as well as the organization's approach for mitigating or managing these risks.

3. Collect Data

Gathering sensitive data is made easier within a respectful workplace culture, particularly one in which diversity is valued and sharing concerns or reporting incidents that occur in the workplace is supported.[2] Further, corporate transparency and demonstrated reliability in the management of sensitive data promotes trust and a willingness to provide consent. This starts with limiting data collection to information that is necessary. In the collection of sensitive data, individuals are able to control the amount and nature of information they wish to share. Exceptions are limited and include data that is needed for employment purposes, such as for payroll where, for example, one's date of birth date is often requested.

2 Through, for example, relevant policies and procedures, trauma-informed approaches and/or a positive reporting culture.

Managing Access to Sensitive Data

If sensitive data is being collected, plans for its management, storage and destruction are also needed. Each of the following factors should be considered, ensuring alignment with company policies and regulatory requirements for privacy.

1. Data Access

All sensitive information, including EDI data, are typically encrypted and accessed under multi-factor authentication. Various types of sensitive data are classified and accessed only by authorized users on a clear, distinct need-to-know basis. Examples of data classification include public, internal, confidential or restricted. Access to sensitive data should be on a strict 'need to know' basis and reviewed regularly as people, roles and data management methods/technology often change.

2. Storing the Data

To ensure safekeeping, sensitive information should be encrypted and stored using current and approved methods only. Secure, cloud-based storage with multi-factor authentication is currently the preferred approach. Effective practice regarding the creation of paper or duplicate copies is to avoid or limit them, and if they are permitted on a temporary basis, protect them with the same rigour as the original copy.

Regularly reviewing stored information for relevance and according to company data retention policies helps to reduce both the costs and risks of unnecessarily storing sensitive information. In keeping with records retention regulations and organizational policy, destroy data once it is no longer useful to the original collection purpose and not required for archival/retention purposes.

3. Destroying the Data

Data no longer relevant to the organization is typically reviewed by a data retention specialist and then destroyed per company data retention and destruction procedures.

Risks Associated with Sensitive Information Sharing

For compliance purposes, mining companies operating in Canada may consult Canadian federal law (PIPEDA[3]), provincial/territorial requirements as well as human rights/employment equity legislation when establishing processes for managing and gathering sensitive information, particularly in relation to employment-related objectives. Companies that operate in other countries may also review privacy laws in those regions and assess their applicability.

To establish a comprehensive information management plan, companies identify the risks of sharing sensitive information, including inadvertent sharing through, for example, human error or relaying information related to a small dataset, and how any requests for sensitive information will be handled. An information breach can result in significant personal and professional risk to individuals as well as financial, legal and reputational risks for an organization.

Continuous Improvement

To create a safe, transparent and dynamic information management system, offer individuals opportunities to raise questions and/or provide feedback on the data collection process. Also consider consulting with a privacy expert on the process to ask for feedback and explore ways to optimize the collection process.

References

GDPR.eu. (2023). *Complete Guide to GDPR Compliance.* https://gdpr.eu/

Office of the Privacy Commissioner of Canada. (2018). *PIPEDA Legislation and Related Regulations.* https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/

Office of the Privacy Commissioner of Canada. (2018). *Summary of Privacy Laws in Canada.* https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/

3 See https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/ for more information.