HAPPY PRIVACY WEEK, CANADA! 3RD EDITION

Posted on January 24, 2024

Categories: Insights, Publications

Nearly every organization will collect, use, share and store the personal information of employees. Much of this information, including financial, health and even biometric information, is considered sensitive and must be handled with great care.

Depending on the province(s) where its employees are located, whether its employees are members of a union, and whether the organization is federally or provincially regulated, an organization may be subject to various laws regarding the processing of its employees' personal information.

Data Privacy Week offers a great opportunity to ensure that your organization's privacy compliance program adequately addresses risks to your employees' data.

McMillan's Top 5 Tips for Taking Control of Employee Data

1. **Monitor Your Employee Monitoring.** Emerging technologies, together with permanent hybrid or fully remote working arrangements, have contributed to a rise in the use of employee monitoring tools, including GPS trackers, biometric timekeeping solutions, video and audio recording, email and network surveillance, and more. These tools may be helpful in verifying employees' location, managing attendance, tracking employee productivity, and monitoring the use of company-owned technology or equipment, among other uses. However, just because these technologies are available does not mean that their use will comply with applicable Canadian privacy laws in all cases. Employee monitoring initiatives must be designed and deployed in a manner that ensures compliance with all applicable legal requirements, including (without limitation) with an eye to limiting the collection and use of employee personal information to what is necessary for reasonable purposes that are appropriate in the circumstances, and ensuring that all required notices and/or policies have been provided and retained. Organizations that use, or are intending to use, employee monitoring tools may consider conducting a privacy impact assessment prior to design and implementation to identify privacy risks and implement appropriate mitigation measures.
2. **Be Selective About Service Providers.** Many organizations engage service providers or vendors who handle employee personal information on their behalf, including payroll providers, employee benefits administrators, human resources consultants, and more. In many cases, employers retain responsibility

for employee personal information when it is processed by third parties, meaning that misuse or mishandling of employee data by a service provider can give rise to significant legal risks, in addition to damaging employee morale. Vendors that process personal information should be carefully vetted to ensure they have appropriate privacy and cybersecurity practices in place to comply with applicable privacy laws and safeguard the personal information they handle. Such vendors must also be subject to appropriate contractual measures to provide a comparable level of protection to employee data. Finally, ongoing oversight and auditing of the vendor's compliance with privacy laws and their contractual commitments may be required.

3. **Limit Internal Access to Employee Data.** Organizations should limit access to employee personal information to those who need to use this personal information to perform their specific job functions. For example, sensitive information about an employee's disability and accommodation request should generally only be available to a select subset of personnel within the organization who require access in order to give effect to the accommodation request. Including this information as part of a more broadly available personnel file can raise the risk of employee snooping and misuse of this information, among other risks. Likewise, organizations should ensure that access to departing employees' personal information is limited to those personnel who will need access on a go-forward basis, for example to respond to any potential legal claims or complaints or to demonstrate compliance with statutory recordkeeping requirements.
4. **Design DEI Initiatives With Care.** A number of organizations collect and use employee personal information with the goal of assessing the need for and developing, implementing and tracking the efficacy of diversity, equity and inclusion initiatives within their workplaces. Though these initiatives are generally well-intentioned, they can raise a host of privacy and security concerns and considerations, particularly involving the collection, use and protection of sensitive employee personal information, such as data about employees' race, ethnicity, religion, disability, sexual orientation, gender identity or expression, and more. Privacy and/or human rights legislation may limit the circumstances in which this information can be collected and how it may be used and disclosed. These limitations should be evaluated and incorporated into the design and implementation of all DEI initiatives, and a plan should be in place to ensure the safeguarding of this information in a manner appropriate to its sensitivity.
5. **Implement Data Minimization.** Employee data should not be stored indefinitely. Accumulating large amounts of data, particularly with respect to former employees, gives rise to a number of risks, including the potential for misuse and costly data breaches. It is important for organizations to develop detailed data retention schedules that take into account any applicable statutory retention periods (such as obligations to retain data to demonstrate compliance with tax and employment standards legislation) while providing for the secure deletion (or anonymization, where permitted by applicable law) of such

information when appropriate.

McMillan's Privacy and Data Protection Team provides practical guidance to organizations regarding their processing and protection of employees' personal information. Celebrate Data Privacy Week by reaching out to your McMillan advisor to discuss strategies for balancing employees' rights with your organization's operational needs!