DEI Initiatives And Data Collection: Navigating Privacy Risks In The Workplace

This is the final installment of our three-part series on Technology & Privacy Law in the Workplace. In this post, we explore Diversity, Equity, and Inclusion ("DEI") initiatives and the potential privacy risks associated with collecting and using employee data.

The commitment to initiatives addressing the equal and inclusive representation of employees in the workplace has continued to grow since 2020 and includes approaches such as countering systemic discrimination, reducing barriers, addressing talent acquisition or employee retention concerns, and managing legal risks.

Often, DEI initiatives start with the collection of employee data. Any time an employer is dealing with employee personal information, they must take into consideration privacy legislation that governs the collection, use and disclosure of such information. In BC, there is legislation that governs the private sector, the *Personal Information and Privacy Act* ("PIPA"), as well as the public sector, the *Freedom of Information and Protection of Privacy Act* ("FIPPA"). The collection of personal data under PIPA is consent-based, however it must only be used for "reasonable purposes." Under FIPPA, personal data collection must be directly related to and necessary for a program, necessary for the purpose of planning or evaluating a program, or expressly authorized by other legislation.

The data required for meaningful DEI initiatives often contains personal and sensitive employee data, which may even relate to protected grounds under the BC *Human Rights Code*. This requires organizations to be diligent, intentional and deliberate when collecting, using or disclosing such data. When approaching DEI initiatives in the workplace, employers should first explore why the data is being collected and what they hope to achieve by collecting the data. Depending on whether data collection is to analyze the demographic of a particular organization, to better understand hiring patterns, or to inform future action plans, the reason for the data collection should inform how and what data is being collected.

Employers should next consider how the data is being collected. Helpful questions for employers to consider at this stage of data collection may include:

i. whether the collection is anonymous or voluntary;
ii. if anonymous, whether the pool of data is small enough that certain employees may be easily identified, potentially leading to privacy breaches;

iii. if neither anonymous nor voluntary, whether the data collection aligns with PIPA's consent requirement;
iv. whether it will be best to use aggregated data or disaggregated data;
v. who should collect the data, and whether best practice would require data collection by a third party, or with the use of consent forms.

Once employers have considered why and how they will be collecting the required data, it is then important to consider how the data will be stored. Inadequately stored data, whether in hardcopy or electronic format, introduces the risk of avoidable privacy breaches. Data, especially employee's personal data, must be stored securely to protect against unauthorized access, unintentional disclosure and theft.

While DEI approaches to work culture often bring a welcome change, they also have the potential to introduce challenges along the way if employers are not careful. To avoid unnecessary privacy breaches, or possible human rights concerns, employers must be intentional, methodical and informed any time they collect, use or disclose employee data.

The content of this article is intended to provide a general guide to the subject matter. Specialist advice should be sought about your specific circumstances.

Authors: Andrea Raso, Catherine Repel, Debbie Preston, John Soden, Scott Lamb, Jeff Holowaychuk, Monica Sharma, Simon Wu

Clark Wilson LLP