5 Traps to Avoid When Handling Employee's Personal Information

As an HR manager, you're entrusted with sensitive personal information about your employees. In addition to undermining employee privacy, inadvertent leaks of that information can expose your organization reputation to liability and compromise your own professional standing. With that in mind, here are 8 traps to watch out for, courtesy of a new Privacy Commissioner of Canada fact sheet based on real-life cases.

1. **Sending Info to the Wrong Recipient**

Trap: Accidentally sending an employee's personal information to unintended recipients is a common cause of Privacy Commission complaints. Example: Mary Smith requests a copy of her personnel file; the organization sends the file to her co-worker, Mary Schmidt.

Solution: Measures you can implement to prevent such mishaps include policies and software that require staff to match not just the names but identification numbers of employees before processing their requests for their own personnel files. You should also require supervisory review and approval before release.

2. **The Group Email Cluster Mess-Up**

Trap: Sending sensitive personnel via email to a group of recipients is a sure fire recipe for leaks. Example: "We have seen multiple cases where information about a staffing process has been emailed to all candidates, revealing their names, email addresses and the fact that they were involved in the process to one another," the Commission advises.

Solution: The Privacy Commission advises organizations to ensure use of the "BCC" field for these types of emails.

3. **Not Realizing that the Same Information May Be "Personal" to More than One Employee**

Trap: Information may be private to more than one employee. This is particularly likely in a situation where one employee has accused another of wrongdoing.

Example: Mary Smith files a confidential sexual harassment complaint against her supervisor, Jay Jones. During a staff meeting, Jay discloses Mary's accusation.

Solution: Advise parties involved in investigations and other proceedings that both the accuser and accused have privacy rights and to refrain from disclosure except where advised by the organization.

4. **Failure to Vet Documents Before Disclosing Them**

Trap: Documents may contain personal information that needs to be shielded from disclosure. Example: In response to a request for relevant documents from a labour arbitrator examining the hiring process, HR discloses notes taken about a particular job candidate during the interview, including the fact that she is HIV-positive.

Solution: Before releasing documents involving employment processes, vet the materials and determine whether they contain personal information about job applicants and/or employees that needs to be redacted.

5. **Collecting Too Much Personal Information**

Trap: It may be necessary to collect personal information about individuals to perform HR functions, e.g., medical information to determine if an employee qualifies for sick leave and other benefits. But there are limits to what you can collect. Example: Mary Smith requests family medical leave to care for her Aunt Emma. The organization asks for medical information about not only Aunt Emma but Mary's husband and children.

Solution: Adopt policies stipulating that while personnel may collect personal information about employees and job applicants to carry out HR-related processes, they may collect only the information essential to carry out those processes. Clearly explain what those processes are and the information essential for each.