Four HR Information System Personal Data Pitfalls to Avoid



Data privacy isn't just an IT department imperative. The personal information about employees and job applicants that you use to perform basic HR functions also has liability implications for your company. Privacy compliance isn't about collecting less personal data; it's about keeping less and for less time. To comply, you must incorporate a retention-and-deletion data strategy into your HR Information System (HRIS). Here are four common HRIS pitfalls and how to avoid them.

1. Shadow Archives

Privacy Law: The *Personal Information Protection and Electronic Documents Act* (PIPEDA) and provincial privacy laws require employers to account for the personal data they collect and make it accessible to employees who request it. To comply, you must be able to identify and locate the HR data you possess.

Pitfall: Data gets lost over time as it sits in network drives, team sites, and inboxes. Managers download résumés, investigation notes, and medical emails "for convenience," creating uncontrolled copies outside governed systems. These copies are invisible to deletion workflows and often surface during access requests or litigation.

Solution: To prevent these problems:

- Designate systems of record, such as Application Tracking System (ATS) for recruitment, HRIS for employee files, and case tool for investigations.
- Ban local storage of HR personal data.
- Turn off default download/sync for sensitive libraries.
- Use view-only or time-limited access where feasible.
- Apply auto-expiry to shared locations, such as 12 to 24 months on HR project folders, with owner notifications before purge.
- Run quarterly "find & clean" scans.
- Impose email discipline by routing sensitive workflows to case tools.
- For unavoidable emails, set mailbox retention rules that purge after a defined period and train staff to file into the system of record, not folders.

2. Backups That Never Expire

Privacy Laws: You may only retain privacy-protected employee data for as long as you

need it to perform the function for which you collected it. Once that purpose and justification end, the data must be meaningfully deleted.

Pitfall: The retention schedules you rely on to comply with this requirement may get undermined where IT maintains full, indefinite backups. Thus, even files that get deleted in production live forever in backup images, resulting in illegal retention.

Solution: To avoid perpetual backup problems:

- Implement a tiered backup system that provides for short-term operational backups (e.g., 30 to 90 days) plus longer-term archives with strict expiry aligned to your longest legal requirement.
- Exclude medical/accommodations, disciplinary investigations, and other sensitive HR folders from long-term backups, where feasible, or encrypt and segment them with shorter backup lifecycles.
- Document your backup retention and map it to your HR retention schedule.
- Test restore procedures to confirm that expired data isn't recoverable after its retention period.

3. Vendor Noncompliance

Privacy Law: Employers are responsible for ensuring that the third-party vendors and service providers to whom they entrust personal data comply with privacy laws and may be held liable for retention and other violations they commit.

Pitfall: Most third-party providers keep client company HR data longer than the client does, whether by default or for their own analytics.

Solution: Include express language in the service contract that:

- Limits how long the provider can retain your HR data by category.
- Requires the provider to delete the data when the retention timeline ends (or other deletion triggers occur) and furnish you a certificate of destruction.
- Bans the provider from using your HR data for model training, product improvement, or any other secondary purpose without explicit, documented consent and legal review.
- Requires the data to be exported in a usable format and verifiably purged within a specific number of days after the contract terminates.
- Gives you the right to audit and/or receive screenshots, reports, completed questionnaires, or other evidence of the provider's compliance with retention schedules and deletion requirements.

4. Mixing Need-To-Know Personal Data into General Employee Files

Privacy Laws: Medical records, functional abilities forms, accommodation requests, disciplinary investigation results, and other employee information handled by HR is especially sensitive and requires extra privacy protection, including strictly limiting access to those who "need to know."

Pitfall: Need-to-know HR data may get saved in general personnel files or find their way into email threads that unauthorized personnel can access.

Solution: Create a segregated repository for sensitive records consisting of separate modules, restricted drives, or case tools with role-based access. Other measures:

- Store only the personal data necessary to perform the HR function.
- Use standardized forms to collect personal data that capture minimal, relevant information, and route directly to the secure repository (rather than email).

- Provide for access logging and periodic review of who accessed what data and why.
- Remove stale permissions immediately.