

# Recordkeeping vs. Privacy Breach – Ask the Expert



Privacy legislation and retention requirements vary from jurisdiction to jurisdiction, and it is best to keep your ducks in a row to avoid any possible breaches of personal employee information.

## **QUESTION**

Our business is currently putting together a personal information retention checklist that captures the requirements under employment standards and CRA and balancing with privacy legislation's requirements to delete identifiable personal information. We are looking for some guidance on whether keeping this information would be deemed a breach of privacy legislation in both BC and Alberta.

## **ANSWER**

### **Employment Standards & CRA Retention Requirements**

Per the CRA, payroll records must be kept for six years from the end of the last tax year to which they relate. Records include name, address, SIN, pay information, deductions, and T4 slips. This is the longest mandatory retention period, and overrides shorter retention periods under other legislation.

Both BC and Alberta require employers to retain payroll and employment records for a minimum of three years after employment ends.

*BC: Employment Standards Act, s. 28(1) – payroll records must be kept for 2 years after the employment ends.*

*Alberta: Employment Standards Code, s. 15 – records must be kept for 3 years from the date the record was made.*

Practically, most employers align with CRA's 6+1 year requirement for consistency.

Both provinces are governed by their Personal Information Protection Acts (PIPA) (separate from the federal PIPEDA):

- Organizations must retain personal information only as long as necessary to fulfill the identified purposes or to comply with legal/regulatory requirements.

- Once the legal purpose has expired, personal information must be destroyed, erased, or made anonymous.

To comply with both privacy and retention rules:

- Document your retention schedule clearly, linking each category of information to the legal basis and retention period (e.g., payroll → CRA → 6+1 years).
- After the retention period, delete or anonymize sensitive personal information (e.g., SIN, addresses, performance records).
- Retain a minimal record (name, job title, dates of employment) for legitimate business purposes.
- Keep this in a separate, access-controlled historical register.
- Note the purpose (e.g., “to verify past employment or organizational history”).
- Include this practice in your privacy policy or retention schedule to demonstrate compliance with PIPA’s accountability principle.

**Do not retain SIN numbers or other government-issued IDs beyond legal retention periods. Limit access strictly to HR or records personnel.**

## **EXPLANATION**

In short:

No – retaining just name and position of former employees beyond statutory periods is not considered a privacy breach, provided you have a documented purpose and safeguard the data. It’s common and permissible to maintain a “former employees directory” or organizational history record that has been stripped of sensitive information.