

BC Employers' Fall Outlook: *Location, Immigration, Personal Information & Termination*

Employment & Labour Law Conference
The Vancouver Club
Thursday, October 13, 2022

CLARK WILSON

Speakers:

Andrea Raso, Partner
Catherine Repel, Associate
Debbie Preston, Associate

Scott Lamb, Partner
John Soden, Associate
Pu Zhang, Immigration Consultant

OUTLINE

1. Privacy Law: What Employers Need to Know
2. Work Permits for Foreign Workers
3. Remote Work: Which Laws Govern?
4. Remote Work – Important Issues
5. Terminations

Privacy Law: What Employers Need to Know

Scott Lamb, Partner

604 643 3103

slamb@cwilson.com

CLARK WILSON

What is Privacy Law in Canada?

- Broad range of concepts, legislation and case law
- Rapidly evolving and growing body of law



Federal Privacy Legislation

Personal Information Protection and Electronic Documents Act (PIPEDA):

- January 1, 2004
- Federally regulated industries (banks, telecoms, airlines)
- Inter-provincial and international exchange of personal information
- Provinces who have failed to pass their own similar privacy law

Provincial Privacy Legislation

British Columbia

Alberta

Quebec

Healthcare Sector:

Saskatchewan

Manitoba

Ontario

New Brunswick

Nova Scotia

Newfoundland and Labrador

BC Privacy Legislation

Personal Information Protection Act (PIPA)

- January 2004
- Personal information within British Columbia



Ten Principles

1. Accountability

- An organization shall designate an individual to be accountable for compliance

2. Identity Purposes

- The purposes for which personal information is collected shall be identified

3. Consent

- The knowledge and consent of the individual are required except where appropriate

Ten Principles

4. Limiting Collection

- The collection of personal information shall be limited to that which is necessary for purposes identified

5. Limiting Use, Disclosure and Retention

- Personal information shall not be used or disclosed for purposes other than those for which it was collected.
- Personal Information shall be retained only as long as necessary for the fulfillment of those purposes

Ten Principles

6. Accuracy

- Personal information shall be accurate, complete and up-to-date.

7. Safeguards

- Safeguards shall be used appropriate to the sensitivity of the information.

8. Openness

- An organization shall make readily available to individuals specific information about its policies and practices.

Ten Principles

9. Individual Access

- An individual shall be informed of the existence, use and disclosure of their personal information.
- The individual shall be given access to the information and be able to challenge the accuracy and completeness of it and have it amended as appropriate.

10. Challenging Compliance

- An individual shall be able to address a challenge concerning compliance to the designated individual responsible for compliance in the organization.

Express Consent vs. Implied Consent

Sliding scale



Express Written Consent
(Health Information)

Implied Consent
(Billing)

Exceptions to Consent

- Collection clearly in interest of individual and consent cannot be obtained in timely way
- Necessary medical treatment and individual is unable to give consent
- Compromise availability or accuracy of personal information and collection is reasonable for investigation or a proceeding
- Performance or sports events open to public

Exceptions to Consent (cont'd)

- Public source (i.e. business contact information)
- Receipt of honour or award or selection for athletic or artistic purpose
- Credit reporting agency and consent was obtained at original collection for disclosure
- Authorized by law
- Facilitate collection or payment of a debt
- Providing legal services to third party

Employees and PIPA

- Special rules for regulating privacy for employees
 - PIPA
 - Employees include volunteers



Employees and PIPA

- Covers starting, managing or ending of an employment relationship:
 - no consent required to collect use or disclose “employee information”,
 - but you must give prior notice to employee before doing so – and explain purpose of doing so

Employees and PIPA

- **What is “employee information”?**
 - personal information about an individual that is collected, used or disclosed solely for the purposes reasonably required to establish, manage or terminate an employment relationship ...”
 - Human Resources activities (e.g. letters of applications, results of interviews, personal references, performance reviews, letters of resignation, termination documents, disability claims and benefits)

Employees and PIPA

- **Retention of “employee information”**
 - If organization makes a decision using employee personal information that directly affects an employee, you must keep the information used for that decision for 1 year
 - Otherwise, the organization must destroy the personal information once the purpose for which it was collected is no longer served by keeping it and retention is no longer required for legal or business purposes

Employment Monitoring

- Video monitoring
- Monitoring software
- GPS tracking
- Biometrics



Employment Monitoring

General Test

1. Is the monitoring necessary for a legitimate or “reasonable” purpose of managing the employment relationship (e.g. past safety or security incidents)?
2. Is the information collected necessary to meet the legitimate purpose?
3. Were less privacy invasive alternatives considered and would they be effective?
4. Were employees given notice of the monitoring and is there a policy governing the use, retention and safeguarding of information collected?

Breach Notification

- Mandatory for PIPEDA
- Recommended for PIPA (soon to be mandatory)
- Many personal information breaches are by employees and not third party hackers

Breach Notification

Do you need to Report all breaches to The Privacy Commissioner?

- Not all breaches must be reported
- But you must report breaches to the individuals concerned and to the Privacy Commissioner if:
 - it is reasonable to believe there will be a “real risk of significant harm to the individual”

Breach Notification

“Significant harm” means “humiliation, damage to reputation or relationships and identity theft” (loss of employment, loss of business or professional opportunities, negative effects on credit record and financial loss)

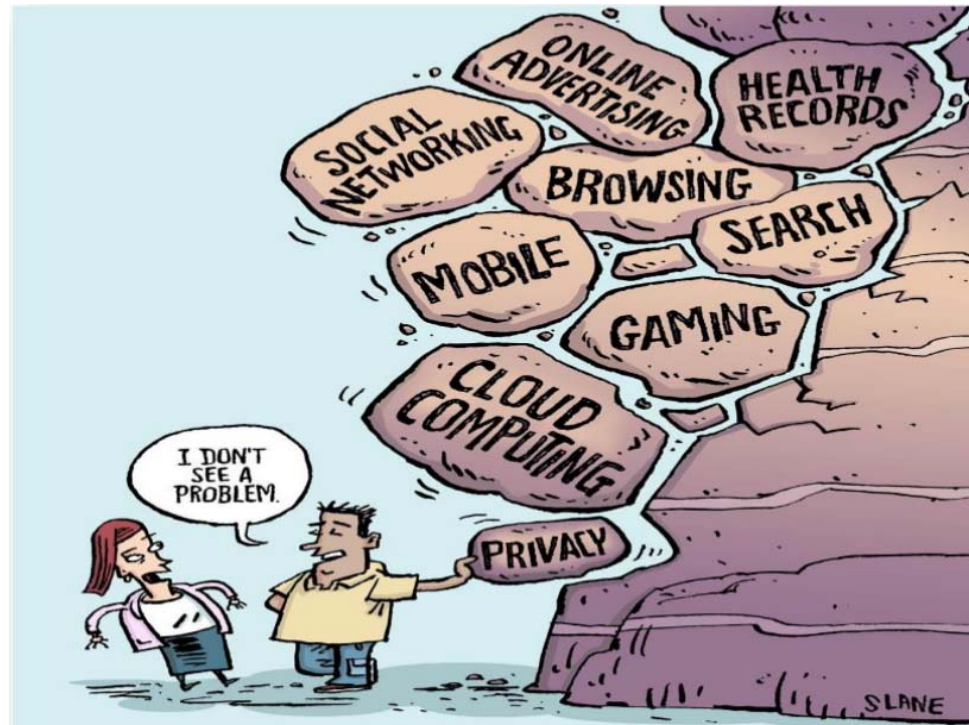
“Real risk” means considering the “sensitivity of the information” and the probability of misuse”

Breach Notification

- Notification to be given in prescribed form “as soon as feasible” after determination of breach to allow individual to:
 - understand significance of breach to them; and
 - take steps, if possible, to reduce risk of harm
- Fines up to \$100,000 per violation under PIPEDA

Privacy Management Programme

PIPA expressly requires organizations to develop and follow policy and practices that are necessary to meet PIPA obligations



Privacy Management Programme

Privacy policies should address the following, at a minimum:

- The purposes for collection, use and disclosure of personal information, including requirements for consent and notification
- Access to and correction of personal information
- Retention and disposal of personal information
- Responsible use of information and information technology, including administrative, physical and technological controls and appropriate access controls
- A process for responding to privacy complaints

Privacy Management Program

Principal elements of a privacy management program:

- Resources for the development, implementation and monitoring of privacy controls
- Institute applicable policies and procedures
- Training delivered regularly
- Information incident management processes
- Compliance monitoring
- Chief Privacy Officer – regular reporting to executive

Privacy Impact Assessments (PIAs)

- Identify purpose or directive of initiative
- Identify personal information to be collected, used or disclosed (how and who)
- Confirm personal information is necessary for the purpose of the initiative
- Identify risks and risk responses proportionate to identified risks
- Identify reasonable security arrangements against such risks (storage)
- Accountable personnel in organization

What's New in Privacy Law

- **Reform of Federal Law**
 - Bill C-27 replaces PIPEDA with new *Consumer Privacy Protection Act* (CPPA)
 - Same framework as PIPEDA
 - Modernize in line with international standards (EU-GDPR and California – CPA)
 - Implement new law 2023?
- **Reform of BC Law**
 - Special Committee of BC Legislature – 34 recommendations
 - Modernize in line with Federal and international standards;
 - Introduce proposal amendments in 2023?

Significant Changes in CPPA

Enforcement

- Privacy Commissioner given enhanced powers
- Privacy Commissioner conducts inquiry after investigating complaint or non-compliance with agreement
- Privacy Commissioner renders decision – if contravention of CPPA:
 - Issue a compliance order
 - Recommend Tribunal impose penalty

Significant Changes in CPPA

Enforcement (cont'd)

- Tribunal has power to impose penalty of up to \$10 million or 3% of gross revenue, whichever is higher
- Tribunal can also award penalty of up to \$25 million or 5% of gross revenue where organization:
 - knowingly contravened breach reporting and notification
 - knowingly contravened requirements to retain personal information that is subject to access request
 - knowingly used de-identification information to identify an individual
 - knowingly contravened a compliance order
 - obstructed Privacy Commissioner in an investigation, inquiry or audit

Significant Changes in CPPA

Private Right of Action

- Where Privacy Commissioner finds a contravention of CPPA
- Class Actions



Significant Changes in CPPA

Enhanced Consent

- Organizations must provide in plain language information to individuals that they would reasonably be expected to understand:
 - purposes of collection, use and disclosure of personal information;
 - manner in which personal information is to be collected, used or disclosed;
 - reasonably foreseeable consequences of collection, use or disclosure of personal information;
 - specific types of personal information involved; and
 - names of any third parties or types of third parties to which personal information may be disclosed.

Significant Changes in CPPA

No Consent Required – Business Activity

- Similar to EU GDPR, organizations may collect or use personal information without consent or knowledge of the individual for specified business activities where the activity is:
 - necessary to provide a product or service requested by the individual from the organization;
 - necessary for the organization's information, system or network security;
 - necessary for the safety of a product or service that the organization provides; and
 - other prescribed activity.

Significant Changes in CPPA

No Consent Required – Business Activity (cont'd)

- But, organizations relying on this exception must only collect or use personal information without consent or knowledge where:
 - a reasonable person would expect the collection or use for such an activity; and
 - the collection or use is not for the purpose of influencing the individual's behaviour or decisions.

Significant Changes in CPPA

No Consent Required – Legitimate Interest

- Also similar to EU GDPR, organizations may collect or use personal information without consent or knowledge if it is for the purpose of an activity in which the organization has a legitimate interest which outweighs any potential adverse effect on the individual and:
 - a reasonable person would expect the collection or use for such an activity; and
 - the collection or use is not for the purpose of influencing the individual's behaviour or decisions.

Significant Changes in CPPA

No Consent Required – Legitimate Interest (cont'd)

- But, prior to collecting or using personal information on the basis of a legitimate interest activity, the organization must:
 - identify any potential adverse effect on the individual that is likely to result;
 - identify and take reasonable measures to reduce effects that will occur or to mitigate or eliminate them
- This personal information assessment (PIA) must be available to the Privacy Commissioner

Significant Changes in CPPA

No Consent Required – De-identified Information

- An organization may use an individual's personal information without their consent or knowledge to de-identify the personal information
- An organization may use an individual's de-identified personal information without their consent or knowledge for the organization's internal research, analysis or development purposes

Significant Changes in CPPA

No Consent Required – De-identified Information (cont'd)

- An organization may disclose an individual's de-identified personal information if it is de-identified before disclosure is made and the disclosure is made to:
 - government institution in Canada;
 - healthcare institution, post-secondary educational institution or public library in Canada;
 - an organization under Canadian law or by contract with a government institution in Canada to carry out a socially beneficial purpose; or
 - prescribed entity.

Significant Changes in CPPA

No Consent Required – De-identified Information (cont'd)

- Socially beneficial purpose is one related to:
 - health;
 - provision or improvement of public amenities or infrastructure;
 - protection of environment; and
 - prescribed entity.

Significant Changes in CPPA

De-identify or Anonymize

- “**De-identify**” means to modify personal information so that an individual cannot be directly identified from it, though a risk of the individual being identified remains
- “**Anonymize**” means to irreversibly and permanently modify personal information, in accordance with generally accepted best practices, to ensure that no individual can be identified from the information, whether directly or indirectly, by any means
- In line with EU GDPR, CPPA does not apply to anonymized personal information

Significant Changes in CPPA

Right to Disposal

- Individuals have the right to have their personal information permanently and irreversibly deleted upon request unless:
 - disposal would result in personal information about another person and the information is not reversible
 - requirements of federal or provincial law or reasonable contracts prevent disposal
 - information is necessary for the establishment of a legal defence or exercise of legal remedies
 - information would have undue adverse impact on accuracy or integrity of information necessary to provide a product or service (and is not in relation to a minor)

Significant Changes in CPPA

Right to Disposal (cont'd)

- the request is vexatious or made in bad faith; or
 - the information is scheduled to be disposed under the organization's retention policy and it makes known the period of time for retention (and is not in relation to a minor)
- Right to disposal is not a general right to de-indexation or a right to be forgotten:
 - issue of impacts to third parties
 - conflicts with freedom of speech and creates issues of censorship

Significant Changes in CPPA

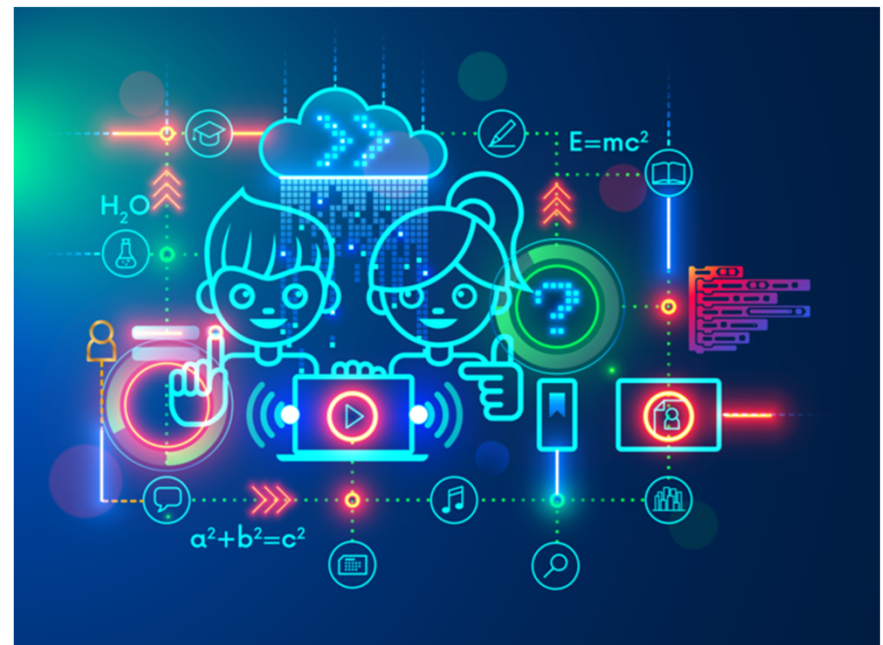
Outsourcing

An organization may transfer personal information to a service provider without consent or knowledge of the individual where the organization ensures by contract or otherwise that the service provider provides a level of protection of the personal information equivalent to that which the organization is required to provide the individual under CPPA

Significant Changes in CPPA

Minors

- A minor's personal information is deemed to be sensitive
- Parents/Guardians are authorized to exercise the rights and recourse under CPPA on behalf of their child (including consent)
- But, a child may object to authorization if they are capable of doing so



Significant Changes in CPPA

Automated decision systems

- Provisions apply where an organization has used an automated decision system to make a prediction, recommendation or decision about an individual that could have a significant impact on them
- then, the organization must, on request by the individual, provide an explanation of the prediction, recommendation or decision that indicates:
 - type of personal information used;
 - the source of the information; and
 - the reasons or principal factors that led to the prediction, recommendation or decision.

Artificial Intelligence (AI)

- **New legislation:** *Artificial Intelligence and Data Act (AIDA)*
 - concerned with wider risks to individual rights that use of AI systems present
 - identifies “high-impact systems” (not defined)
 - requirement to identify, assess and mitigate the risks of harm or bias
 - requirement to monitor compliance with mitigating measures
 - significant fines for contraventions: greater of \$10 million or 3% of an organization’s annual gross global revenues

Work Permits for Foreign Workers

John Soden, Associate

604 643 3148

jsoden@cwilson.com

Pu Zhang, Immigration Consultant

604 891 7783

pzhang@cwilson.com

CLARK WILSON

What do Employers and Foreign Workers Want?

1. Highest chance of success
2. Minimum delay
3. Best value for money



How do We Achieve Those Outcomes?

1. Highest chance of success -

A. We require detailed information and documents on the:

1. Employer;
2. Employee; and
3. Occupation.

B. We evaluate 1 – 3 against the eligibility criteria of potential immigration programs

C. We choose the program best aligned to 1 to 3

How do We Achieve Those Outcomes?

2. Minimum delay -

- A. Wherever possible we make applications at a Port of Entry (“POE”)
- B. We Request two-week processing at a visa office if not eligible for POE application
- C. We Include documentary evidence to prove all eligibility criteria are met

3. Best value for money –

- A. $1 + 2 = 3$

Golden Rules

- If possible Avoid the Temporary Foreign Worker Program (TFWP)
- Always provide relevant documentary evidence – immigration decisions are made on the balance of probability
- Help the immigration officer to make the decision you want by making the application easy to navigate and read



Clark Wilson LLP – TOP FIVE

We use the following programs regularly because they are aligned to the needs of our client base:

**#1
Mobilité
Francophone**

**#2
Intra-Company
Transferees**

**#3
Free Trade
Agreement
Professionals**

**#4
Significant Social,
Cultural &
Economic Benefit**

**#5
International
Experience
Canada**

#1 Mobilite Francophone

- No LMIA required
- Clearly defined eligibility criteria to be met:
 - Habitual language of use is French;
 - NOC O, A and B occupations;
 - All provinces / territories other than Quebec.
- Often enables POE application

#2 Intra-Company Transferees

- No LMIA required
- Clearly defined eligibility criteria to be met:
 - Intra-company relationship between foreign employer and Canadian employer;
 - Employment relationship between foreign employer and employee;
 - NOC 0, A and B occupations;
 - Senior management, functional management and specialized knowledge categories.
- All provinces and territories, including Quebec
- Often enables POE application

#3 Free Trade Agreement Professionals

- No LMIA required
- Clearly defined but some different eligibility criteria:
 - Limited to specific occupations;
 - Education credentials specified; and
 - Work experience is specified.
- All provinces and territories, including Quebec
- Often enables POE application

#4 Significant Social, Cultural & Economic Benefit

- No LMIA required
- This is our fall-back program
- A highly discretionary program. Must prove employment of foreign national will created significant benefit for Canada
- Recent successful examples include:
 - AI scientists;
 - Engineers; and
 - Senior managers in Community Contribution Companies (“**CCC’s**”).

#5 International Experience Canada

- No LMIA required.
- Often known as the “working holiday program”
- Clearly defined eligibility criteria but specific to each participating country
- Not all countries are eligible



Regulatory Changes

New IRCC regulatory requirements for employers of foreign workers -

1. Make information about their rights in Canada readily available;
 2. Provide signed employment agreement – English or French
 3. A workplace free of abuse and/or reprisals
 4. No fees to be charged to employee for recruitment services; and
 5. Make reasonable efforts to provide employees with access to health services if injured/ill in the workplace
- IRCC will conduct audits/inspections
 - A range of administrative & financial penalties will be applied

Remote Work: Which Laws Govern?

Andrea Raso, Partner

604 891 7761

araso@cwilson.com

Provincial Employment Standards Legislation

Generally:

Provincial
Employment
Standards legislation
applies to work
performed in a given
Province.



Employment Standards

However, remote or teleworking may blur the lines of where the work is being performed



Employment Standards

What does the legislation say?

NB: Act applies notwithstanding that the work or services may be performed in whole or in part outside of New Brunswick.

Ont: Act applies to the employees working within Ontario, and outside Ontario to the extent that the work outside Ontario is a contract of work performed in Ontario

Employment Standards

The rest of the Provinces' legislation, including BC, is silent with respect to the applicability of their respective legislation outside of the Province.



Case Law

Zhang v. IBM

- Software developer working out of IBM's Toronto office
- Zhang requested to work from home
- Agreement entered into allowing IBM to terminate the arrangement at its discretion and Zhang would have to return to a traditional work environment

Case Law

Zhang v. IBM

- Zhang moved to BC and worked there for 2 years
- IBM notified him to return to Ontario and work in the Ottawa office
- Zhang returned to Ottawa but said he would return to Toronto office
- IBM gave him ultimatum and deemed him to have resigned when he refused

Zhang v. IBM

Labour Board held:

For the Ontario Act to apply, there must be some back and forth between Ontario and elsewhere, and not a move from one province to another with only a possibility of some future return to Ontario.

Likely a similar result in BC.

Other Considerations

- International work
- Tax issues
- Human rights
- Privacy laws

Choice of Laws

SO:

1. Consider choice of laws in contract so both parties understand which laws apply, but be mindful that the law may dictate a different jurisdiction.
2. Know the employment standards differences in the jurisdiction where the employee is remotely working as there are key differences, e.g. employees in Nova Scotia cannot be terminated without just cause after 10 years of employment

Remote Work: Important Issues and Things to Consider

Catherine Repel, Associate

604 643 3175

crepel@cwilson.com

Employment Contract Issues

- The employment contract needs to reflect the arrangement that is (or is going to be) in place
- Things to consider:
 - Is this remote work temporary?
 - Is this remote work agreed upon?
 - Do you want to retain the ability to have the employee come into the office?
 - For existing employees, what does their employment agreement currently say about where work is to be performed?

Health and Safety and Workers Compensation

- Employers have health and safety obligations for employees working remotely
- Employees must have a safe workspace for remote work, with proper ergonomic considerations
- Employers are responsible for workplace incidents and injuries for remote workers, e.g. employee working from home on a work call dropped their pen and herniated a disc they picked up the pen – coverage allowed
- There are protocols and procedures for check-ins if a worker is working alone or in isolation

Accommodation Issues

- Employers have human rights obligations to employees working remotely
- However, depending on the protected ground that is engaged, the obligations will be different
- Consider the issue and protected ground engaged, for example:
 - Childcare/family responsibilities
 - Disability

Privacy, Security and Confidentiality

- Ensure appropriate security measures in place for employees working remotely
- Confidential information treated appropriately and kept secure
- Secure equipment and systems
- Monitoring of employees

Working Hours and Availability

- Clear expectations around start and end times
- Clear expectations about availability and responsiveness
- Ensure employees not adjusting schedules or working overtime
- Be proactive

Office Expenses

- Employers are responsible for reimbursement for certain office expenses for remote employees



- *BC Employment Standards Act:*

An employer must not require an employee to pay any part of the employer's business costs except as permitted by the regulations

Policies

- Employers should have policies in place for remote work that touch on all areas covered:
 - Health and safety
 - Accommodation
 - Privacy, security and confidentiality
 - Work hours and availability
 - Expenses



Terminations

Debbie Preston, Associate

604 891 7779

dpreston@cwilson.com

CLARK WILSON

Terminations

With Cause – No requirement to provide notice or pay in lieu

Without Cause – Must provide notice or pay in lieu

- Employees are entitled to at least the minimum notice period set out in the *Employment Standards Act*
- May be entitled to common law notice if there is no valid employment contract

Terminations – Without Cause

Things to Consider:

1. Written employment contract?
 - i. Is it enforceable?
2. Possibility of human rights complaint/other liabilities?

Terminations – To Do

➤ Two letters:

- ✓ First letter sets out the termination and pay in lieu of notice, if applicable
- ✓ Second letter sets out a “without prejudice” offer in exchange for signing a release
 - You cannot get a Release for providing *only* minimum standard or employee entitlement under their employment contract



Termination - Release

- MUST provide gratuitous amount in exchange for signing Release;
- Can't use bonus if employee arguably already entitled to that bonus;
- Can't use pay in lieu of notice;
- Try to ensure employee has time to review Release before signing, not signed on the same day.



Termination - Release

Termination vs. Release



- Termination doesn't have to be agreed to by employee
- Release is a legal document that records employee's agreement to relinquish their right to any future claim
- Employee doesn't have to agree to Release

Termination - Release

How Does a Release Operate?

- Does not bar employee from commencing a claim;
- Creates a way to dispense of a claim;
- Terms may be negotiated by employee;
- Can include various other provisions aimed at employee's post-termination actions:
 - Non-disparagement clause;
 - Confidentiality clause;
 - Restrictive covenants.

Terminations - Reminders

1. No notice/pay in lieu required where:
 - Employee is terminated with cause; or
 - Employee has been employed for less than 3 months.
2. Cannot terminate employee who is on leave;
3. Final wages (regular wages, overtime, statutory holiday pay, etc...) must be paid within 48 hours after the date of termination.

Questions?



Andrea Raso

Partner

604 891 7761
araso@cwilson.com



Scott Lamb

Partner

604 643 3103
slamb@cwilson.com



Catherine Repel

Associate

604 643 3175
crepel@cwilson.com



John Soden

Associate

604 643 3148
jsoden@cwilson.com



Debbie Preston

Associate

604 891 7779
dpreston@cwilson.com



Pu Zhang

Immigration Consultant

604 891 7783
pzhang@cwilson.com

These materials are necessarily of a general nature and do not take into consideration any specific matter, client or fact pattern

CLARK WILSON