IAPP CANADA
Privacy Symposium 2019

Designing an Employee Privacy Program

Speakers

David Longford, Chief Executive Officer, DataGuidance by OneTrust

Lyndsay A. Wasser, CIPP/C,
Co-Chair, Privacy & Data Protection
Co-Chair, Cybersecurity, McMillan LLP

Oxana Iatsyk, CIPP/C, General Counsel, Privacy Officer and Corporate Secretary, Ruby Life Inc.

Outline

I. Welcome and Introductions
II. Designing a Global Program
III. The HR Lifecycle; from Application to Exit
IV. Monitoring - Challenges posed by tech / innovation
V. Panelists' Perspectives
VI. Questions and Answers
VII. Closing Remarks

Designing a Global Program

- Challenges
  - Balancing different legal regimes (e.g., GDPR versus Canadian laws)
  - Structure versus flexibility
  - Local “buy-in”
- Benefits
  - Positive employee relations

The HR Lifecycle; from Application to Exit

- Background checks, including use of social media
- Managing the Relationship - Rights of candidates, responsibilities of employers
- The post-employment relationship
- Common misconceptions

Monitoring - Challenges posed by tech / innovation

- Video surveillance; GPS tracking; Computer monitoring; Call recording
- Legal bases and contracts
- Proportionality and business drivers
- Awareness and training

Panellists' Perspectives

- How do I begin building an employee privacy programme?
- How do I maintain effectiveness during organisational change?
- Where can it all go wrong?
- What are some regional approaches used by multinationals?

Effective Employee Privacy Program

- Conduct periodic audits of data access, consent and retention practices and compliance
- Address data protection concerns identified during audits
- Conduct periodic mock breach exercises; implement "post mortem" policy revisions
- Review and improve contracts, policies, practices and guidelines, to reflect the evolving legal requirements and case law
- Document changes to policies and procedures
- Report to stakeholders

- Define geographical and corporate governance structure (centralized or distributed)
- Understand organization's composition (union, contractors, employees)
- Identify and review applicable laws
- Locate and review current policies, procedures and practices
- Locate and review current privacy-related communications to employees
- Identify employee data collected, its location, reasons for data processing and extent of data transfers between various company locations
- Identify 3rd party vendors having access to employee data
- Locate and review Offer Letter, Employment and Independent Contractor Agreement templates
- Review current service agreements for the vendors having access to employee data, incl. recruiters
- Identify technologies used to screen and monitor employees
- Identify gaps in privacy compliance

- Limit the scope of personal data collection and processing
- Train and retrain new and current employees
- Track data and access to it, and data processing reasons Track employee consent, training completion, policy receipt acknowledgement, compliance
- Implement and watch adherence to data retention rules
- Respond to employee and third-party privacy-related inquiries within reasonable time
- Audit privacy practices of potential vendors
- Log, review, address and report when necessary privacy incidents, breaches and complaints
- Enforce compliance

- Define an employee privacy roadmap
- Assign responsibilities for data privacy throughout the organization
- Develop training materials
- Draft Data Processing Agreement/contract clauses
- Update internal templates and vendor agreements as necessary
- Advise HR of limits on background checks and employee monitoring
- Communicate and post privacy related notices, policies and guidelines for easy access by employees
- Define and communicate data security-related policies and guidelines, including those re breach notification, and third-party vendor assessment rules

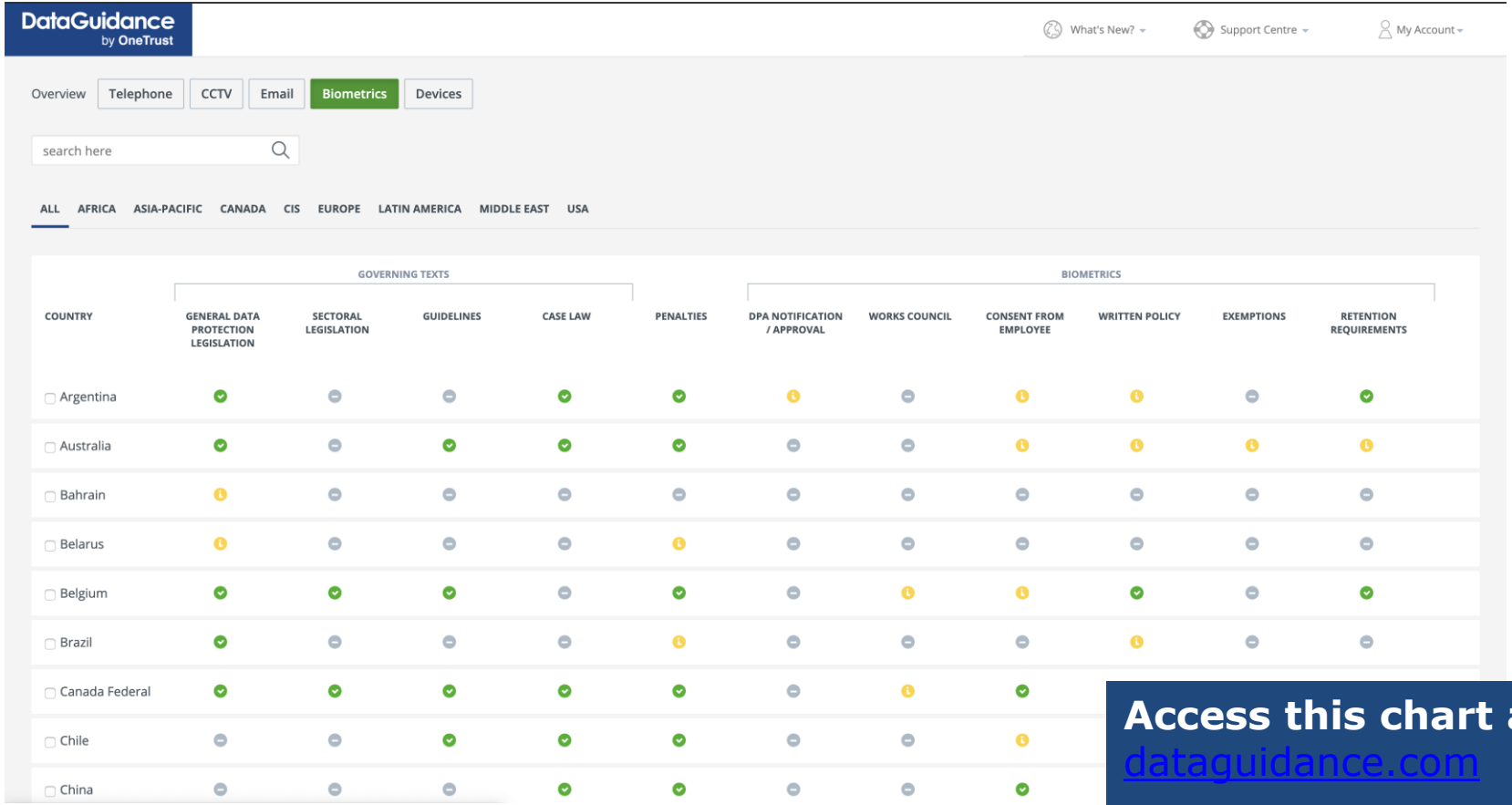
Q & A

Helpful References

Background Checks in Canada

- Federal and Quebec employees – prior consent required
- Alberta and BC employees - advanced notice required
- Risk - possible claim of "intrusion upon seclusion"
- Rule of thumb:
  i. Ensure proper background checks are completed even when 3rd party is engaged (*The Treaty Group Inc. v. Drake International Inc.* (2007) 86 O.R. (3d) 366)
  ii. Limit checks to assessing the employee's suitability for continued or prospective employment
  iii. Failure to consent to background check may give cause for termination of employment (*Covenoho v. Pendylum Inc., [2016], O.J. No. 4498)*

Employee Monitoring Cross-Border Chart



Access this chart at
dataguidance.com

County specific in-depth guidance

DataGuidance by OneTrust

What's New? Support Centre My Account

Back

Canada - Employment

TABLE OF CONTENTS

July 2018

1. INTRODUCTION

1.1. Key legislation and regulations

Protection of employee personal information in Canada varies across jurisdictions. The following legislation applies to private sector employers ('Canadian Privacy Legislation[1]'):

- The Personal Information Protection and Electronic Documents Act 2000 ('PIPEDA'), governs the collection, use, disclosure and protection of employee personal information by federally regulated employers, e.g., banks, inter-provincial transportation, telecommunications, shipping and aerospace;
- The Personal Information Protection Act, SA 2003 c P-6.5 ('Alberta PIPA'), governs the collection, use, disclosure and protection of employee personal information by provincially regulated employers in Alberta;
- The Personal Information Protection Act, SBC 2003 c 63 ('B.C. PIPA'), governs the collection, use, disclosure and protection of employee personal information by provincially regulated employers in British Columbia;
- An Act respecting the Protection of Personal Information in the Private Sector, CQLR c P-39.1 ('the Quebec Act'), governs the collection, use, disclosure and protection of employee personal information by provincially regulated employers in Quebec.

In addition to the above, Manitoba has passed The Personal Information Protection and Identity Theft Prevention

ABOUT THE AUTHORS

Lyndsay Wasser

McMillan LLP

Lyndsay Wasser is a Partner at McMillan LLP, Co-Chair of McMillan's Privacy Group and a Certified Information Privacy Professional/Canada. Lyndsay advises and assists management in all areas of employment, labour, pension and benefits laws, including advising on hiring, performance management, employment standards, human rights laws and employment terminations, as well as drafting or reviewing employment contracts, compensation plans and employment policies.

Lyndsay also regularly advises and assists clients on a broad range of privacy issues, including advising on access requests, privacy breaches, workplace privacy issues, e.g., background checks, computer/video/phone monitoring, GPS tracking, drug and alcohol testing,

Access this information at dataguidance.com

Employee Monitoring Principles

- Necessity
- Finality
- Transparency
- Legitimacy
- Proportionality
- Accuracy
- Retention
- Security

Employee Monitoring Tests

Federal Privacy Commissioner	Alberta Privacy Commissioner	BC Privacy Commissioner	Quebec Privacy Commissioner	Unionized Employees
Is the measure demonstrably necessary to meet a specific need?	Does a legitimate issue exist to be addressed through the collection of personal information?	Can the employer demonstrate that it is reasonable to believe that a breach of an employment agreement has taken place?	Is surveillance necessary in order to manage the workplace?	Is the surveillance reasonable in light of the circumstances?
Is the measure likely to be effective in meeting the need?	Is the collection of personal information likely to be effective in addressing the legitimate issue?	Has the employer given proper notice to employees of its monitoring practices?	Is the surveillance carried out in an arbitrary manner?	Is the surveillance conducted in a reasonable manner?
Is the loss of privacy proportional to the benefit gained?	Is the collection of personal information carried out in a reasonable manner?	Is the collection of personal information reasonable for the purposes of establishing, managing or terminating an employment relationship?	Is the surveillance based on other evidence that already exists against the worker?	Are there any alternatives to the surveillance?
Is there a less privacy-invasive way of achieving the same end?			Is the surveillance conducted in the least intrusive manner possible?	

Effective Employee Privacy Program

- Conduct periodic audits of data access, consent and retention practices and compliance
- Address data protection concerns identified during audits
- Conduct periodic mock breach exercises; implement "post mortem" policy revisions
- Review and improve contracts, policies, practices and guidelines, to reflect the evolving legal requirements and case law
- Document changes to policies and procedures
- Report to stakeholders

- Define geographical and corporate governance structure (centralized or distributed)
- Understand organization's composition (union, contractors, employees)
- Identify and review applicable laws
- Locate and review current policies, procedures and practices
- Locate and review current privacy-related communications to employees
- Identify employee data collected, its location, reasons for data processing and extent of data transfers between various company locations
- Identify 3rd party vendors having access to employee data
- Locate and review Offer Letter, Employment and Independent Contractor Agreement templates
- Review current service agreements for the vendors having access to employee data, incl. recruiters
- Identify technologies used to screen and monitor employees
- Identify gaps in privacy compliance

- Limit the scope of personal data collection and processing
- Train and retrain new and current employees
- Track data and access to it, and data processing reasons Track employee consent, training completion, policy receipt acknowledgement, compliance
- Implement and watch adherence to data retention rules
- Respond to employee and third-party privacy-related inquiries within reasonable time
- Audit privacy practices of potential vendors
- Log, review, address and report when necessary privacy incidents, breaches and complaints
- Enforce compliance

- Define an employee privacy roadmap
- Assign responsibilities for data privacy throughout the organization
- Develop training materials
- Draft Data Processing Agreement/contract clauses
- Update internal templates and vendor agreements as necessary
- Advise HR of limits on background checks and employee monitoring
- Communicate and post privacy related notices, policies and guidelines for easy access by employees
- Define and communicate data security-related policies and guidelines, including those re breach notification, and third-party vendor assessment rules