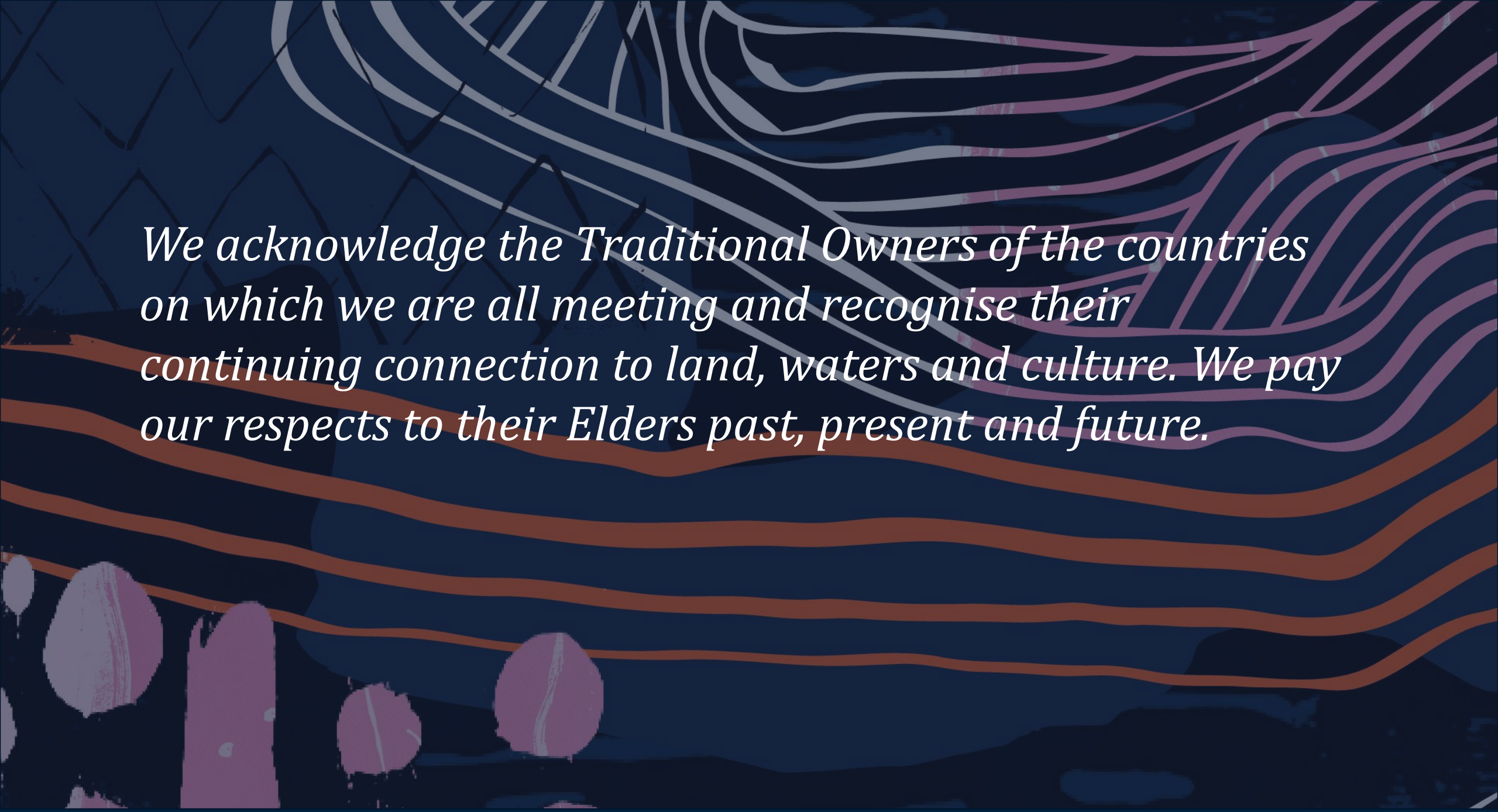
WIN In-House Counsel Week 2026

Employment & Privacy in the Digital Workplace: Risks, Reforms, and Practical Strategies

Presenters:
Sarah Birkett, Mitch Robertson

DLA PIPER

WIN what in-house lawyers need


We acknowledge the Traditional Owners of the countries on which we are all meeting and recognise their continuing connection to land, waters and culture. We pay our respects to their Elders past, present and future.

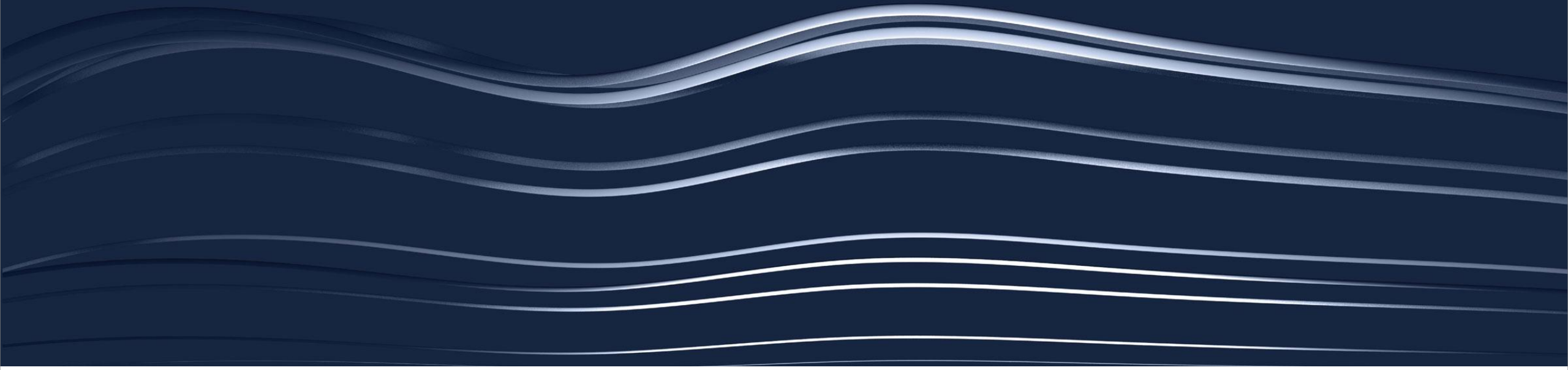
Introduction

Volume of HR data increasing

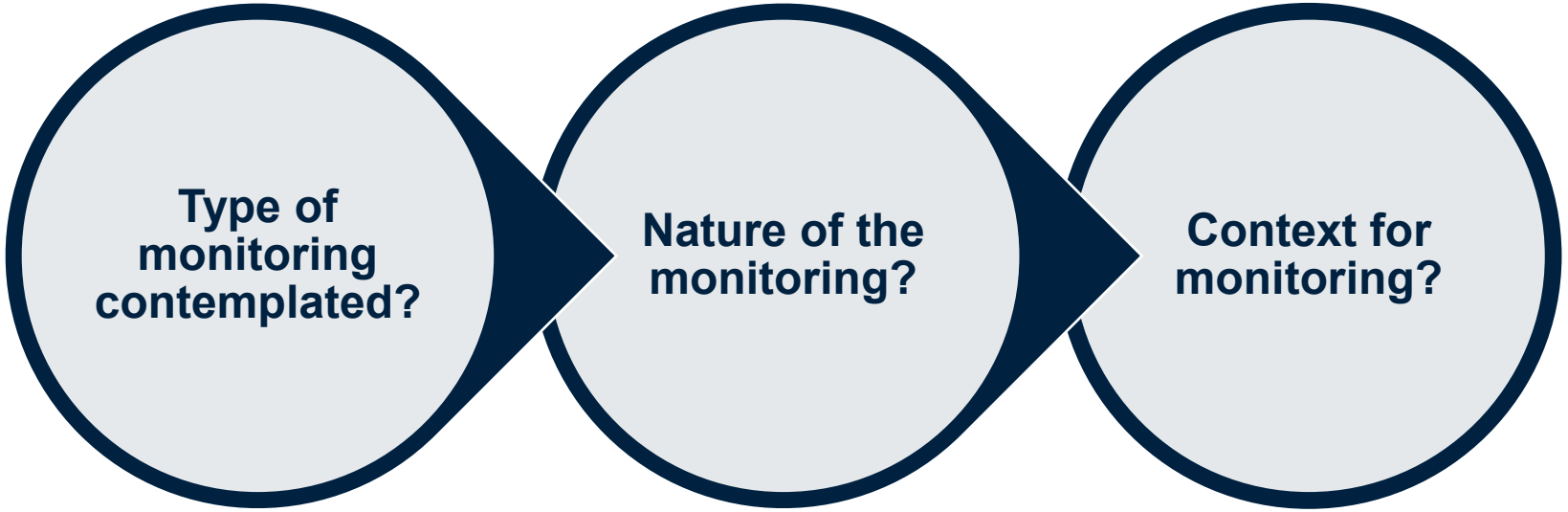
Driven by technology and social changes

Overlapping legal risks

Lawful Workplace Monitoring



Understanding Monitoring



- Remote Work
- BYOD / Company Device
- Productivity Tools
- Time and Attendance Systems

Understanding the context around the monitoring being proposed is critical.

Understanding the law around workplace monitoring

Specific workplace surveillance laws apply in certain States/Territories	More general surveillance device laws apply elsewhere	Types of surveillance
• *Workplace Surveillance Act 2005* (NSW) • *Workplace Privacy Act 2011* (ACT)	• e.g. *Surveillance Devices Act 1999* (VIC), which includes workplace specific provisions in broader surveillance law (e.g. prohibition on surveillance in workplace bathrooms etc.)	• Camera surveillance • Computer surveillance • "Tracking" surveillance (e.g., vehicles and devices) • Email interception

Victoria - Legislative Assembly's Economy and Infrastructure Committee's Inquiry into Workplace Surveillance (May 2025)

New South Wales - *Amendment (Digital Work Systems) Bill 2025*

Compliance Framework – NSW / ACT

Australian Capital Territory

Workplace Privacy Act 2011 (ACT)

New South Wales

Workplace Surveillance Act 2005 (NSW)

Covert – not permissible (other than limited exemptions)

Changerooms / bathrooms – prohibited

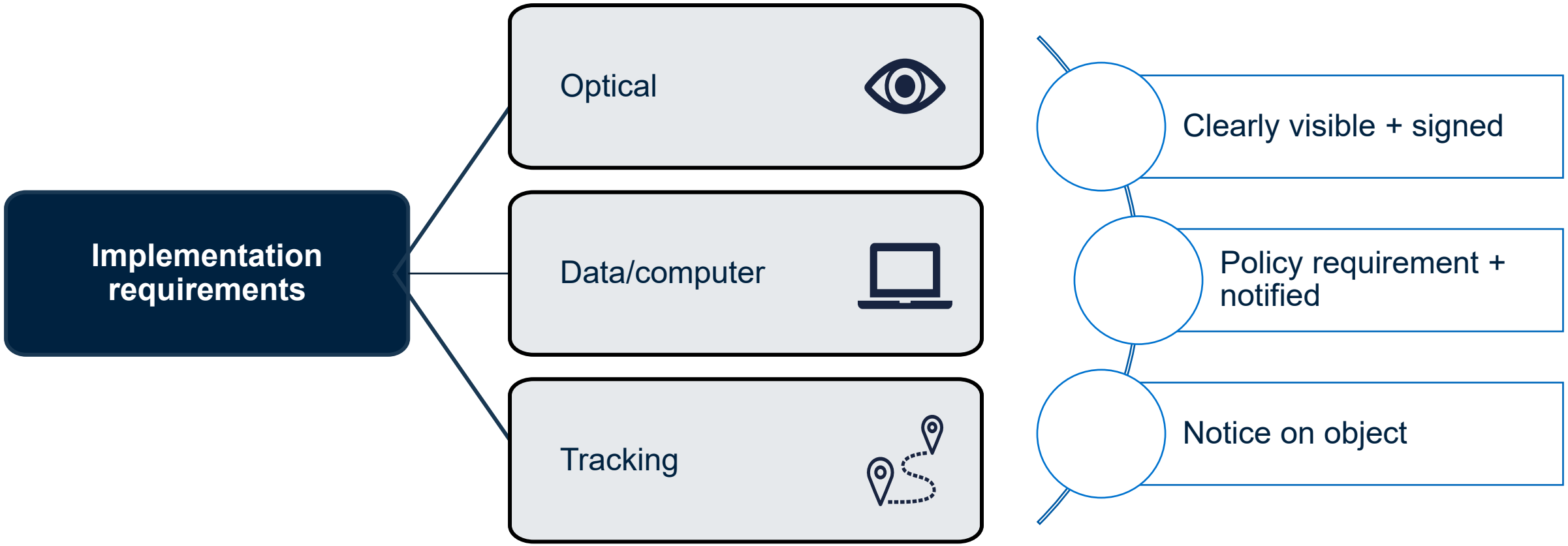
Other surveillance – permissible but must satisfy specific statutory framework

Notification

Implementation requirements (vary depending on device)

Consultation* (ACT only)

Compliance Framework



Intercepting emails → Accordance with policy → Prevented delivery notice (exceptions)

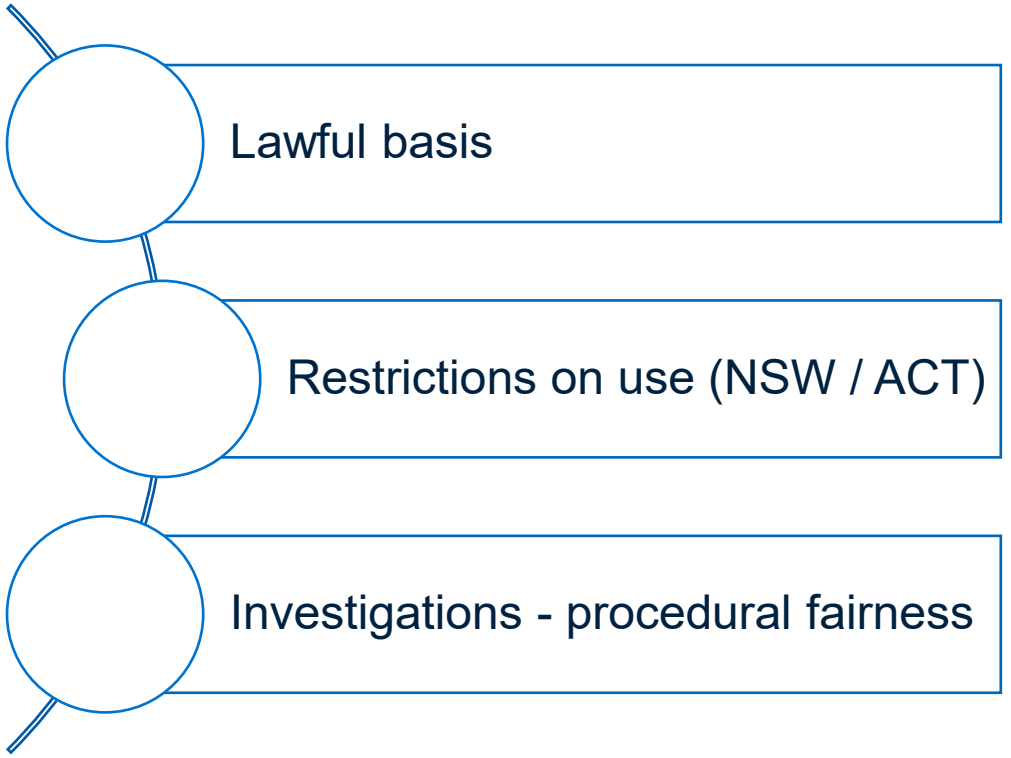
Using the data… limitations and considerations

Performance

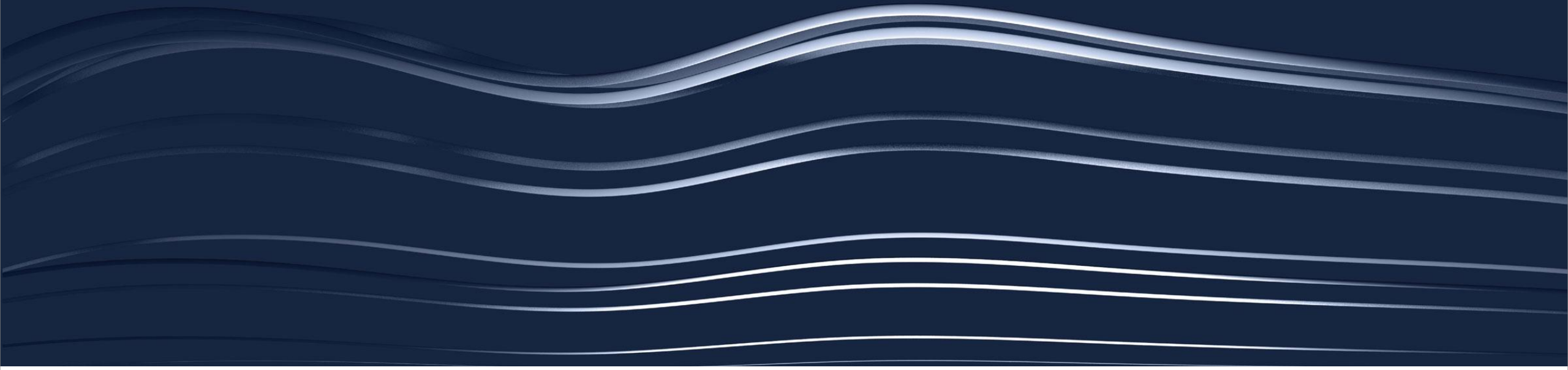
Conduct

Attendance

Security



Workplace Privacy Obligations & Potential Reform



Employee records exemption

- All acts and practices directly related to a current or former employment relationship and employee records are exempt from the *Privacy Act 1988* (Cth)
- Employee records is defined broadly, and so potentially provides blanket exemption
- Known limitations, including:
  - contractors and other individuals engaged by an organisation
  - unsuccessful employment candidates
- Not applicable to Government entities
- Additional rules apply regarding Tax File Numbers

Testing the limits of the exemption

Lee vs Superior Wood [2019]

- Employee records exemption only applies to records once held by the employer (and not up to and including collection)
- Employer's direction requiring employees to consent does not result in consent being “freely given”
- Other options available to Superior Wood to log Lee’s start/end times that did not involve collection of biometric data

ALI and ALJ (Privacy) [2024]

- Case confirms narrow scope of employee records exemption – just because information has some relation to the employee doesn’t mean the information is covered by the employee records exemption
- Disclosure of employee’s health information to the workforce was not “directly related” to her employment, and the health information was not the subject of an “employee record” when the email was sent

Expected reform

Reforms have been "accepted in principle"

Exemption will remain

- Balancing act between the privacy expectations of employees and the realities of the workplace
- Employers must have adequate flexibility to collect, use and disclose employees' information that is reasonably necessary to administer the employment relationship
- Data subject rights and consent requirement specifically identified

Enhanced transparency

- Privacy policies and APP 5 statements
- Should already be in use for recruitment processes

Information security

- Requirement to adopt reasonable technical and organisational steps in APP 11.1
- In practice, controls should already be in place

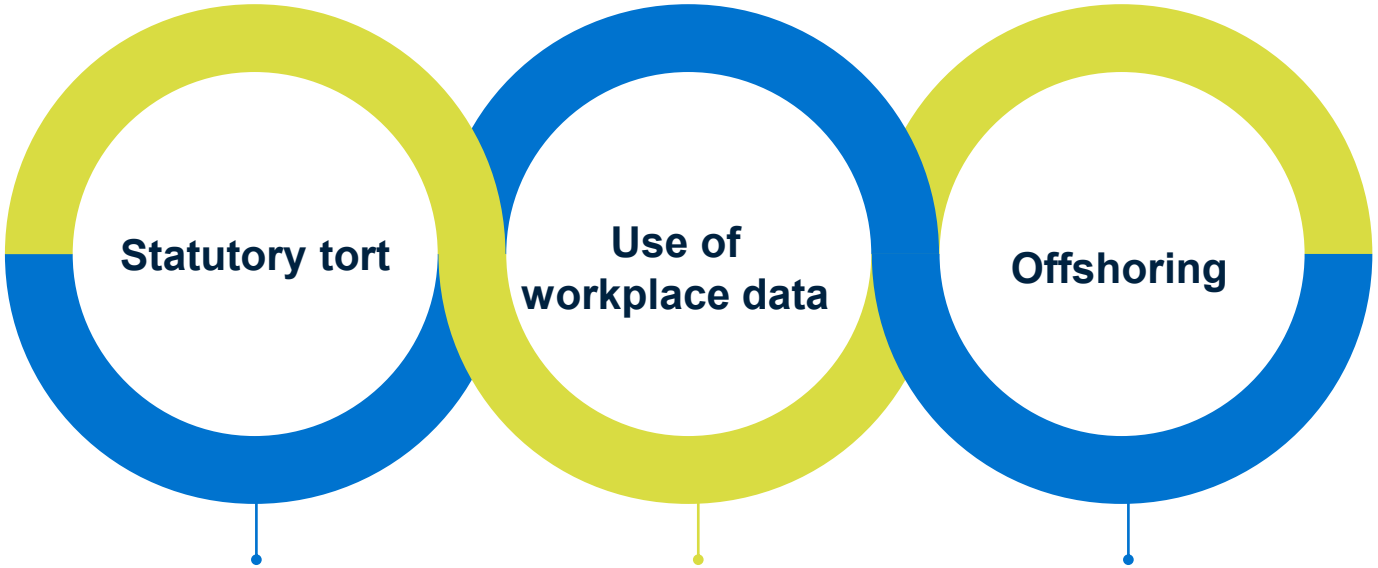
Data retention

- APP 11.2 requirement to destroy/de-identify employee records
- However, would be subject to other laws (including retention requirements in the Fair Work Act)

Data breach notification

- Requirement to notify both the OAIC and affected employees of eligible data breaches
- Separately, 72-hour timeframe for OAIC notifications has been proposed

Other privacy considerations



- Became effective in June 2026
- Statutory cause of action relating to misuse of information or intrusion on seclusion
- Not related to “acts and practices” – no carve out for employee records

- If exemption does not apply (e.g. personal emails), need lawful basis for use under APP 6
- Secondary purpose? Are policies in place?
- Permitted general situations

- Need legal basis for offshoring if exemption does not apply
- In practice, relies upon vendor contract terms and IGDTAs

What is biometric data?

Biometric data is sensitive information if it is:

- part of an automated biometric verification system; or
- a biometric template.

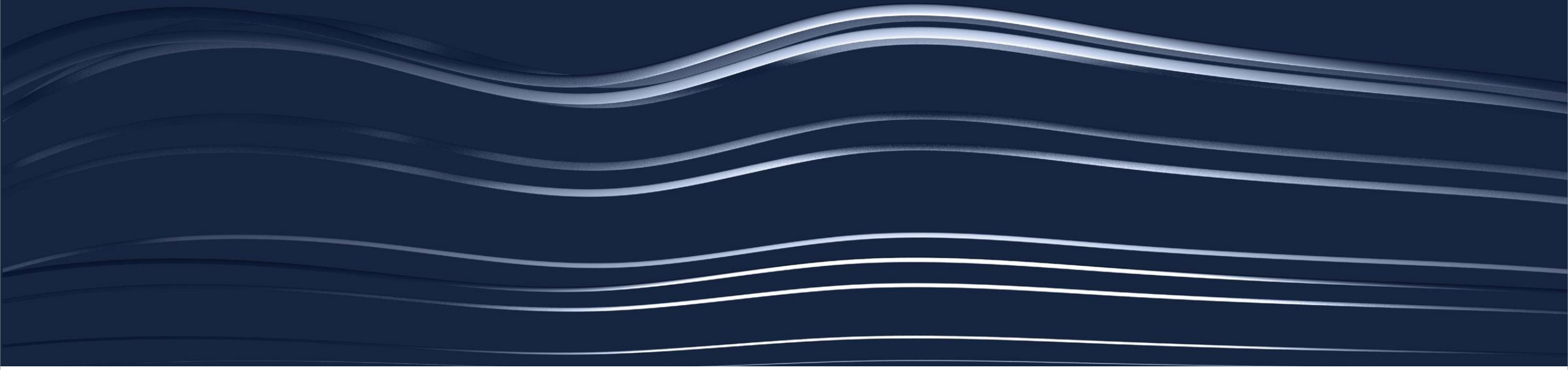
Biometric data can only be collected if:

- the individual has consented;
- the law authorises or requires collection;
- it is necessary to prevent a serious threat to life, health or safety of an individual; or
- another exception applies.

Bring Your Own Devices

- No BYOD-specific laws in Australia
- BYODs are regulated indirectly via existing privacy, surveillance and workplace laws
- Employers should set defined limits and impose necessary information security controls, e.g.:
  - Frequent security patching
  - Require basic safeguards like passwords, screen-locks and updated software
  - No use of public wi-fi
  - Discourage use of unapproved apps (“shadow IT”)
  - Separate work and personal data

Practical Strategies



Managing Risk – Employment

Notification and Communication

Contractual terms

Policies / Transparency

Controls and Governance

Training

Disputes / Managing Concerns

Managing Risk – Privacy

Visibility of processing

Map legal obligations – does anything fall outside the exemption?

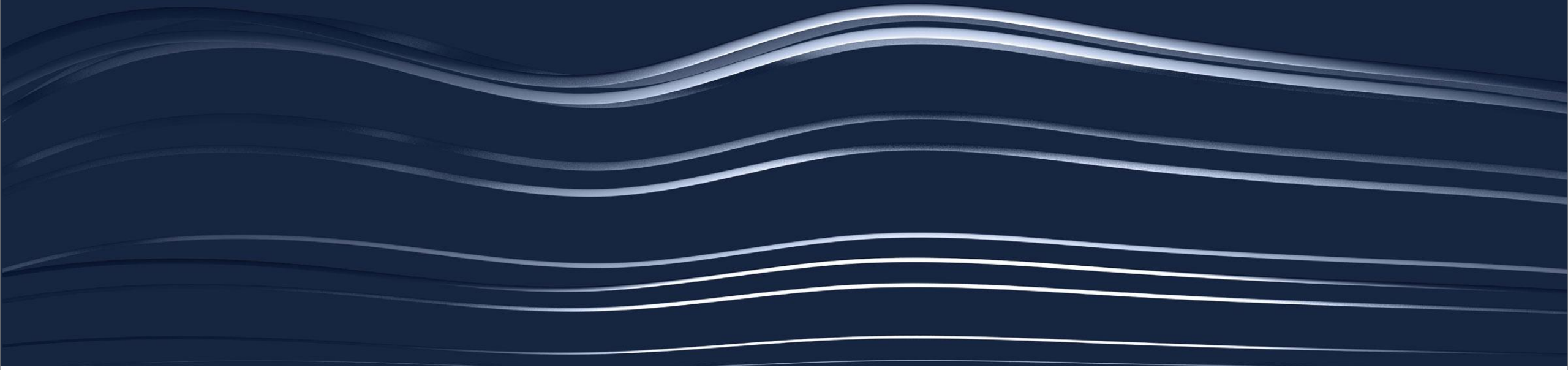
Transparency (whether required or voluntary)

Identify HR supply chain

Training

Incident response processes and staff comms

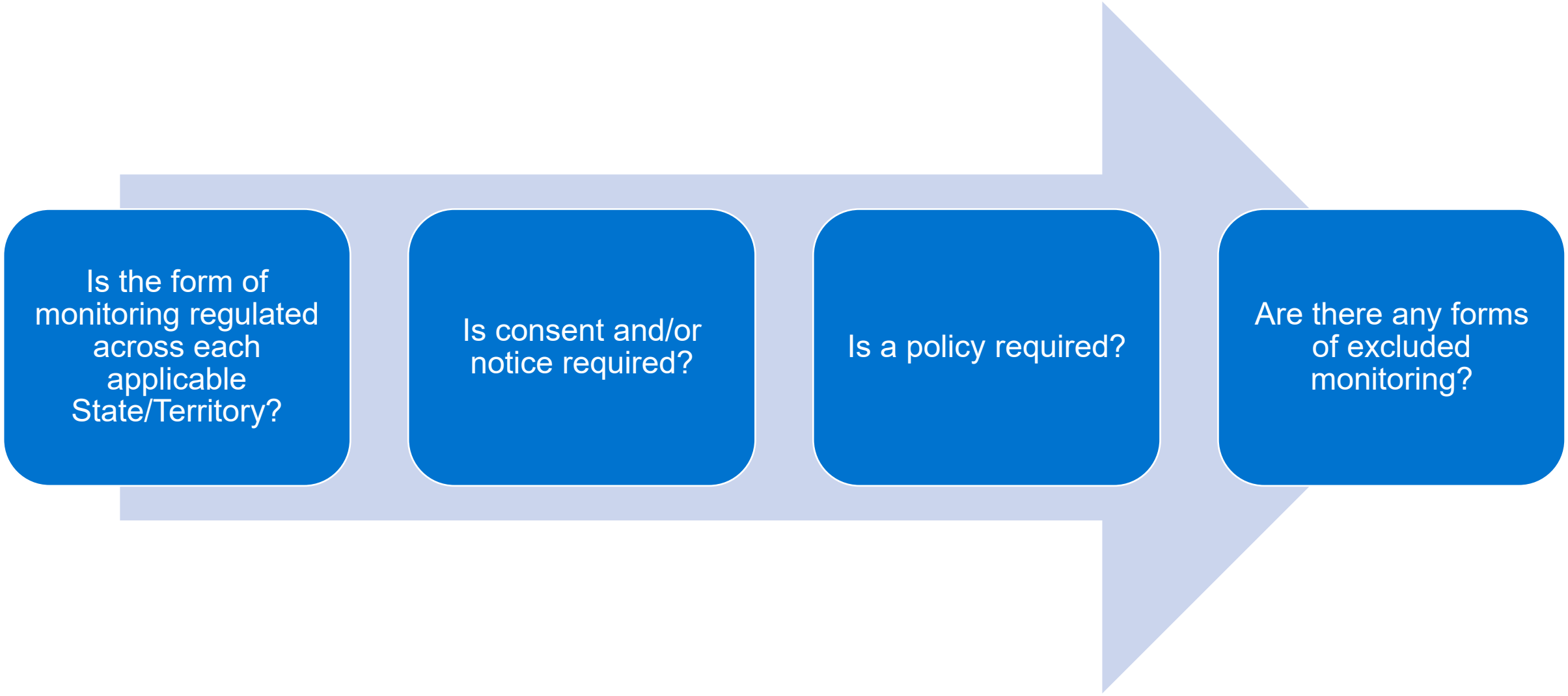
Key takeaways



Checklist – does the employee records exemption apply?

- Are all of the staff current or former employees?
- Do the records relate directly to their employment?
- Are any new/emerging technologies in use?
- What standards do you wish to adopt as an employer?

Checklist - Monitoring



WIN In-House Counsel Week

Thank you for joining our webinar:

Employment & Privacy in the Digital Workplace: Risks, Reforms, and Practical Strategies

Session presenters:

Sarah Birkett
Special Counsel
DLA Piper, Melbourne
T: +61 3 9274 5464
E: sarah.birkett@dlapiper.com

Mitch Robertson
Special Counsel
DLA Piper, Sydney
T: +61 2 9286 8017
E: mitch.robertson@dlapiper.com

Join our WIN program today

www.dlapiperwin.com