Seyfarth

A Global Perspective on DEI Identification

DEI Micro-Webinar Series

Caitlin Lane | Partner
Kathryn Weaver | Partner
International Employment Law

17 September 2024

Seyfarth Shaw LLP

Legal Disclaimer

This presentation has been prepared by Seyfarth Shaw LLP for informational purposes only. The material discussed during this webinar should not be construed as legal advice or a legal opinion on any specific facts or circumstances. The content is intended for general information purposes only, and you are urged to consult a lawyer concerning your own situation and any specific legal questions you may have.

Presenters

Caitlin Lane
Partner, International Employment Law
New York

Kathryn Weaver
Partner, International Employment Law
Hong Kong

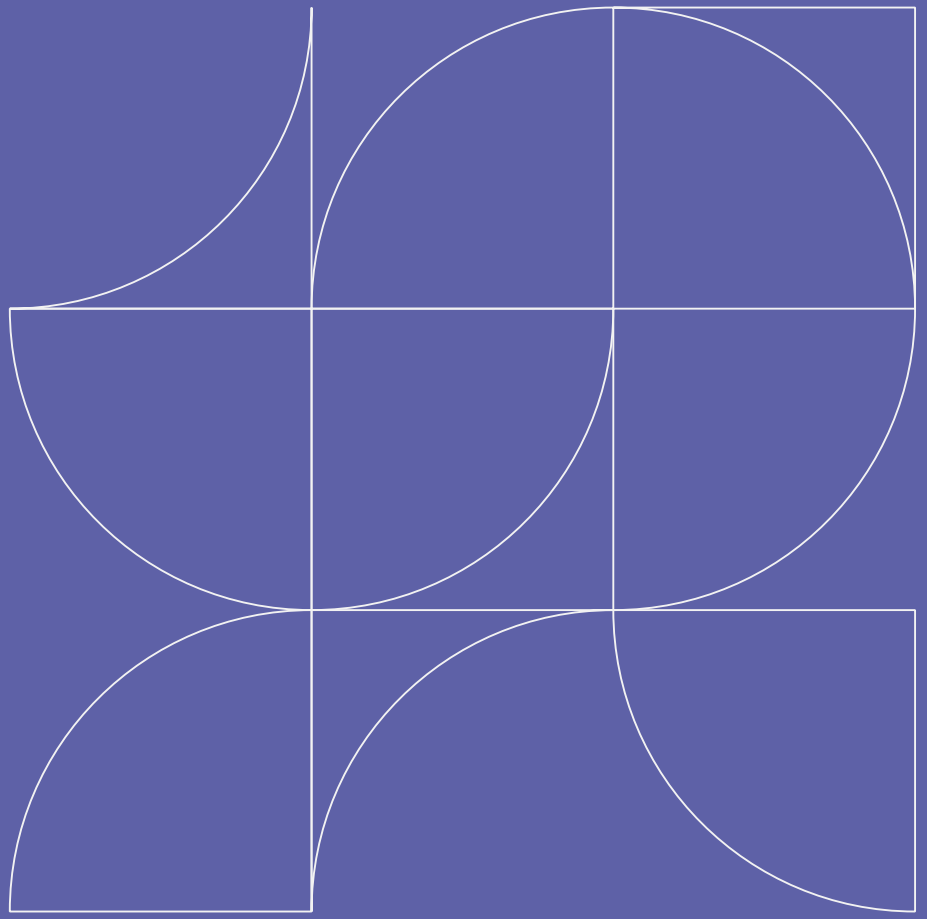
Agenda

1 | Considerations for global organizations

2 | APAC and EMEA approaches to DEI monitoring

3 | Best practices

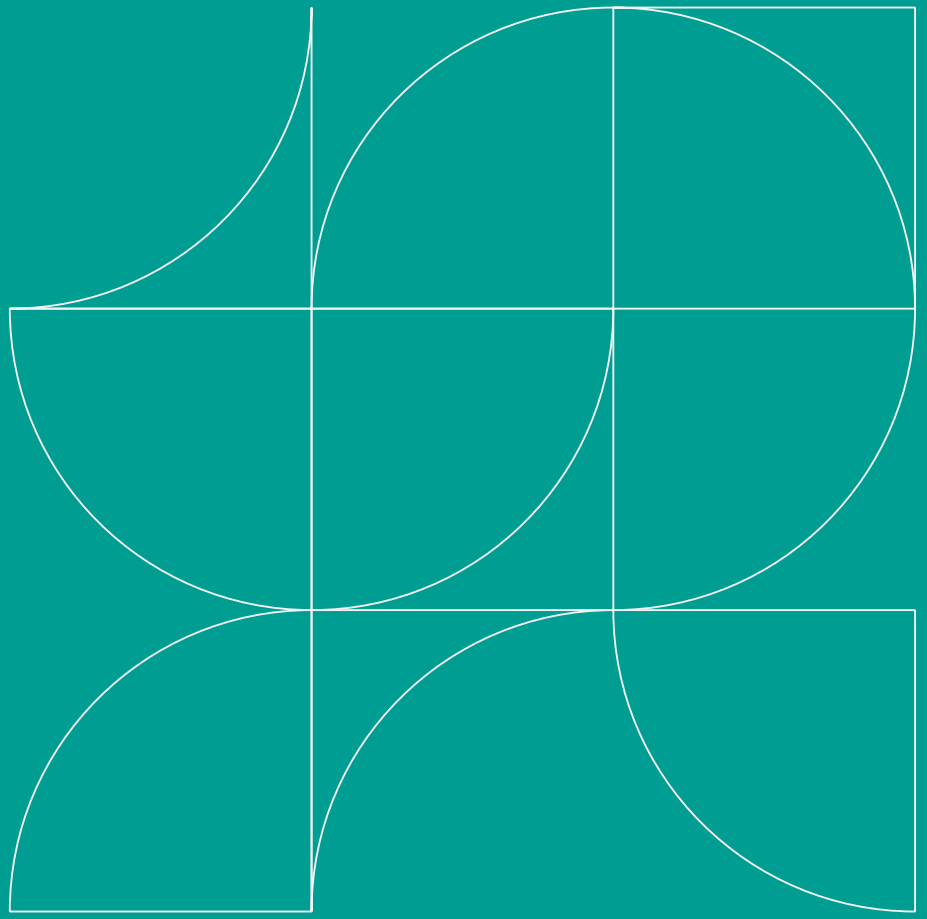
1. Considerations for Global Organizations Rolling Out DEI Monitoring



Overview and landscape

- Global approaches must consider intersection of DEI initiatives and local country and regional laws that impact what data can be collected and how it can be used
- Different rules for applicants vs. employees
- Mandatory obligations (e.g. pay equity / transparency) vs. collection for internal initiatives
- Choosing the right metrics

2. APAC and EMEA Approaches to DEI



What Data Can Be Collected?

APAC

- Before asking what data can be collected, consider why you are collecting it
- Be mindful of data privacy concerns, discrimination risks and cultural sensitivities when planning to monitor DEI data – these differ across APAC
- DEI data often relates to protected attributes – be aware of which attributes are protected in each jurisdiction
- Risk of claims by those who disclose DEI data and then find themselves prejudiced by an employment decision – consider whether positive discrimination is permitted locally
- DEI data provided by applicants/employees, unless anonymized, would constitute “personal data” under local laws
- Some jurisdictions have “sensitive personal data”, which is often afforded greater protection – be aware of which jurisdictions have this and the rules attached
- Examples of sensitive personal data are medical records, genetics, sex life, criminal record, etc.

What Data Can Be Collected?

EMEA

- Under the GDPR, sensitive personal data includes race, ethnic origin, political opinions, religious or philosophical beliefs, genetic data, health-related data, trade union membership, data concerning the person's sex life or sexual orientation.
- Certain data points required to comply with law
- Example: countries with disability quotas
- Non-EU jurisdictions also have data privacy requirements which may vary
- Confirm local position for non-GDPR countries when forming a DEI data collection plan
- Employer watch-out: does the data being collected present a discrimination risk?
- What is being collected? How will it be used?

Is Consent Required?

APAC

- Whether consent is required will generally depend on jurisdiction and whether data is sensitive
- Hong Kong and Singapore do not generally require consent if the conditions within the local data privacy laws are satisfied, including the data subjects being notified of the purposes of collection
- Consent is required in Hong Kong when using personal data collected for one purpose for a new purpose not explained to the data subject originally
- Japan and China require consent when collecting / using sensitive personal data
- In South Korea and India, consent is generally required

Is Consent Required?

EMEA

- Consent to process sensitive personal data under the GDPR may be permissible
  - Can be viewed as invalid due to imbalance of power
- Alternative, preferred approach: to further the legitimate interests of the employer
- In non-GDPR countries, consent likely required unless there is some other legally mandated reason to collect the personal data or local law preference for legitimate interests of the employer

Voluntary vs Mandatory Disclosure

APAC

- Employees should generally be notified if disclosing their personal data is voluntary or a mandatory requirement
- If mandatory, the consequences of not providing it should be explained
- Personal data requested for the purpose of DEI monitoring is often voluntary unless laws/regulations mandate that certain data must be collected
- Voluntarily disclosing personal data regarding certain attributes can be helpful to the employer and employee, e.g., notifying an employer of a disability so the employer can provide reasonable accommodations

Voluntary vs Mandatory Disclosure

EMEA

- Given the limits of what can be collected, particularly in EU countries, consider how to approach data collection
- Voluntary disclosure is likely to allow for a broader range of information to be collected than mandating disclosure
- Example: in most countries an employer can give employees the option to disclose their preferred pronouns
  - Mandating the disclosure of this information would trigger privacy issues
  - May not be culturally appropriate to ask for this data (e.g. ME countries that outlaw or do not recognize same-sex relationships)

Self vs Anonymous Disclosure

APAC

- Anonymized data would generally not constitute personal data and therefore would not be regulated by local personal data laws
- Still good practice to consider why data is being collected and what employer intends to do with it, even when anonymized
- Pseudonymization might be permitted in some jurisdictions, e.g. Japan
- Self-disclosure can enable employers to provide accommodations, support, ERGs, etc – but be mindful of greater discrimination claim risks

Self vs Anonymous Disclosure

EMEA

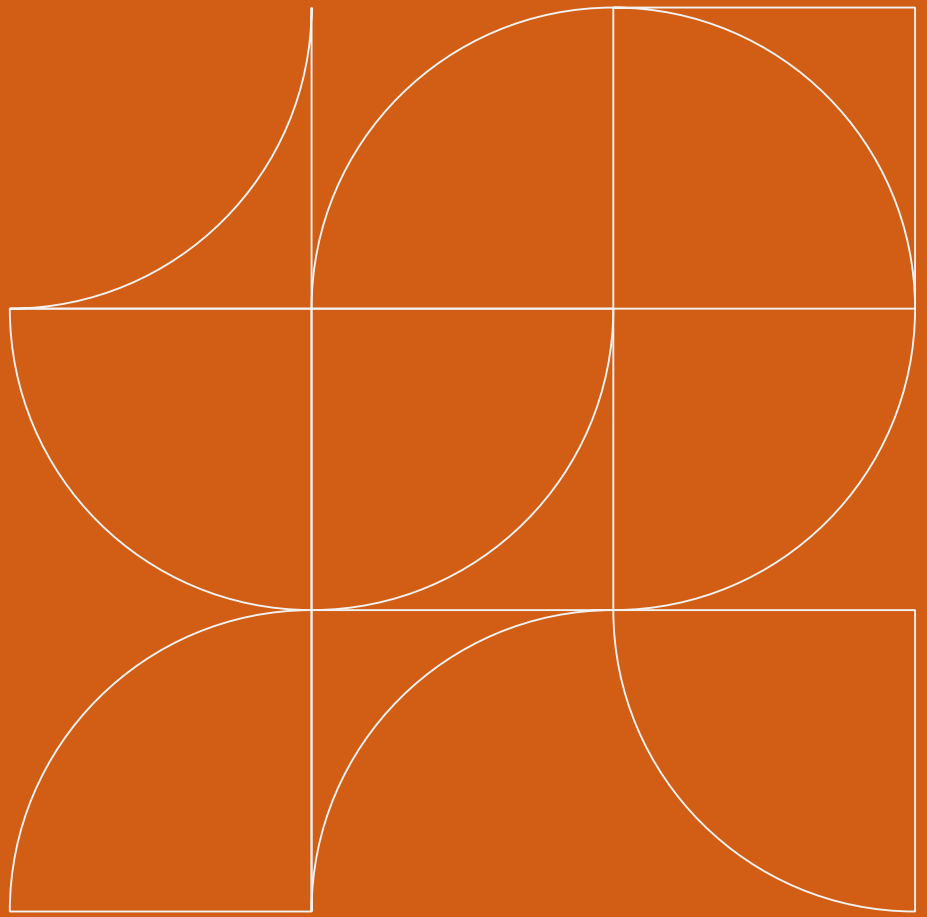
- Anonymized data generally does not constitute personal data and may be the only way to obtain certain data, e.g. race and ethnicity in certain countries
- Range of data that can be collected may be broader if anonymized (particularly if voluntary)
- Consider the company objectives of the data collection
  - Does anonymized data provide enough information for what the company is trying to achieve?

Transfer and Storage of DEI Data

APAC and EMEA

- Transfer: Generally stringent requirements on the cross-border transfer of personal and sensitive personal data, particularly if the receiving country has less rigorous data privacy regulations (e.g., the US)
  - Privacy notices
  - Note China's complex rules on data transfers
- Storage: Personal data must only be stored for no longer than necessary for achieving the purpose of collection, unless local law specifies a longer mandatory retention period

3. Best Practices



Best practices

- Understanding how data will be used can help inform how data is collected
- Tailor data requests to match objectives for data use
- Ensure compliance with data privacy requirements
- Consider cultural norms and sensitivities
  - a one size fits all approach may not be appropriate globally
- Consider anonymizing personal data to reduce data privacy and discrimination law risks
- Consider how data will be stored and whether it needs to be transferred and plan accordingly

CLE: NEW PROCESS

Please scan the QR code and complete the digital attendance verification form to receive CLE credit for this program.

You will need:

1. **Title: DEI Micro-Webinar Series:** A Global Perspective on DEI Identification
2. **Date Viewed:** September 17, 2024
3. **Attendance Verification Code:** SS____

State-specific CLE credit information can be found in the form.

thank you

For more information, please contact:

Caitlin Lane
Partner, International Employment Law
clane@seyfarth.com
+1 212 218 5528

Kathryn Weaver
Partner, International Employment Law
kweaver@seyfarth.com
+852 3956 0616