

# Labour & Employment

## Global Snapshot on Collecting and Monitoring Diversity and Inclusion Data



Businesses are under pressure from a range of internal and external stakeholders to create and maintain genuinely diverse and inclusive workplaces. We know from speaking to our clients that a growing number of employees and candidates expect that businesses “walk the walk” and not just “talk the talk”, clients are increasingly asking for diversity data as part of the pitch process and investors are focusing on an organisation’s diversity and inclusion efforts when making investment decisions.


















It is consequently not surprising that more and more businesses want to collect and track Diversity and Inclusion data about their staff. This may include information about gender, race, ethnic origin, religion, socio-economic background and health which may help them understand the current profile of their workforce, assess the impact of their equal opportunities policies, determine what steps they may need to take to address any barriers to change and measure progress against any objectives/targets set.

As you would expect in light of the very personal nature of some of this information, collecting and making use of D&I data is not always straightforward, especially for businesses looking to do so on a global basis. In some countries, such as the UK, most employees are familiar with requests for D&I data as part of an employer’s diversity and inclusion efforts. In other countries, such requests would be seen as highly intrusive and even unlawful. There are data protection and privacy risks to be addressed, as well as social and cultural barriers to obtaining and using such information.

In this guide, we set out the key questions that employers are likely to encounter about collecting and monitoring D&I data around the world. Lawyers from our global Labour & Employment and Data Privacy teams have provided outline answers to these questions for their particular jurisdiction, including practical tips on how employers may be able to overcome any challenges in this area.

Please note that this guide is intended as a high-level overview only and should not be regarded as a substitute for legal advice. It was last updated on 1 June 2022. We recommend that you always check the latest position with your local labour and employment and data protection lawyers. Where “✓/✗” responses are given, they may be dependent on the facts and specific advice should always be taken.

# Contents

	<b>Australia</b> ..... 4		<b>Russia</b> ..... 22
	<b>Belgium</b> ..... 6		<b>Saudi Arabia</b> ..... 24
	<b>China</b> ..... 8		<b>Singapore</b> ..... 26
	<b>Czech Republic</b> ..... 10		<b>Slovak Republic</b> ..... 28
	<b>France</b> ..... 12		<b>Spain</b> ..... 30
	<b>Germany</b> ..... 14		<b>United Arab Emirates</b> ..... 32
	<b>Hong Kong</b> ..... 16		<b>UK</b> ..... 34
	<b>India</b> ..... 18		<b>US</b> ..... 36
	<b>Italy</b> ..... 20		



# Australia

## Is there a legal requirement on employers to collect/publish D&I data? If so, for what purposes?

**Gender reporting:** The Workplace Gender Equality Act 2012 (Cth) requires employers with 100 or more employees to report annually to the Australian Government statutory agency, the Workplace Gender Equality Agency. The report relates to the following gender equality indicators:

- gender composition of the workforce;
- gender composition of governing bodies of relevant employers;
- equal remuneration between women and men;
- availability and utility of employment terms, conditions and practices relating to flexible working arrangements for employees and to working arrangements supporting employees with family or caring responsibilities;
- consultation with employees on issues concerning gender equality in the workplace; and
- any other matters specified by the Minister.

Employers must submit the report by 31 May each year in order to be compliant, as failing to do so will result in the employer being published in the Agency’s annual report as “non-compliant”.

In addition, employers with 500 or more employees must meet the minimum standards set out by the Minister under Workplace Gender Equality (Minimum Standards) Instrument 2014 (Cth). The minimum standards include having policies or strategies to support one or more of the gender equality indicators and achieve the related objectives.

## Can employers **require** job applicants/staff to provide them with D&I data about themselves?

No, employers cannot insist that individuals provide this personal data.

## Can employers **ask** job applicants/staff to provide them with D&I data about themselves on a voluntary basis?

Yes, however, employers should ensure they do not breach privacy or anti-discrimination laws when doing so.

## Does the information have to be provided on an anonymous basis?

No, although employees may be more encouraged to provide the information when anonymous.

Employers should assess whether conducting anonymous surveys for instance is the best option, as the size of the company or team may undermine anonymity and identify the individual. If it results in the latter, employers will have to comply with the Privacy Act 1988 (Cth) (Privacy Act) and the Australian Privacy Principles (APP) – discussed further below.

## Are there data protection/privacy issues for employers to consider when collecting and monitoring D&I data?

Yes, as such information is considered “personal information” or “sensitive personal information” under the Privacy Act.

**Personal information:** This is defined as information or an opinion (whether or not the opinion is true) about an identified individual, or an individual who is reasonably identifiable. Common examples of personal information include an individual’s name, address, telephone number, date of birth, employment details or references.

The Privacy Act sets out the 13 APP. They include the following requirements:

- information should only be collected by lawful and fair means if it is reasonably necessary for one of the organisation’s functions or activities;
- an organisation can only use or disclose personal information for the purpose for which it was collected (the “primary purpose”) or for a secondary purpose, if an exception applies;
- ensure that the personal information the organisation collects is up to date, accurate and secure; and
- the organisation must provide individuals with access to personal information held about them.

SQUIRE   
PATTON BOGGS  
[squirepattonboggs.com](http://squirepattonboggs.com)