

**Baker
McKenzie.**

**Answering the Call to
Advance ID&E in the
Workplace While Keeping
Privacy in Mind**



Scan QR Code to access
The Employer Report blog

ACC NCR Privacy and Technology Conference | September 13, 2023





Krissy Katzenstein
Baker McKenzie,
Partner

+ 1 212 626 4364
krissy.katzenstein@bakermckenzie.com



Adeola Olowude
Baker McKenzie,
Associate

+ 1 202 835 6245
adeola.olowude@bakermckenzie.com



Alyson Palmer
Google,
Corporate Counsel,
Global Employment



Manisha Reddy
Baker McKenzie,
Associate

+ 1 312 861 8033
manisha.reddy@bakermckenzie.com



Agenda

- 01** Diversity data collection from a US and global perspective

- 02** Pay transparency / pay equity reporting requirements


- 03** Collecting contingent worker ID&E data and tracking supplier diversity

- 04** Disclosing ID&E data: avoiding pitfalls and setting expectations

- 05** GDPR, CCPA and privacy considerations when collecting ID&E data

- 06** Appendix





**01 Diversity data
collection from a US
and global perspective**

Diversity data collection – Level setting



Overall considerations

- Why collect diversity data?
 - Analyze the concrete benefits of current ID&E efforts in the workplace
 - Consider how to have a positive impact on ID&E in the future
 - Share diversity data with stakeholders such as employees and shareholders to remain transparent and accountable
- Collecting diversity data can be risky, expensive and complicated
 - Increases when a company has global operations in different jurisdictions with different rules and regulations
- Important considerations in jurisdictions where collecting so you know what information to collect and measure, or what information to ask employees to volunteer if voluntary reporting
 - Legal restrictions
 - Cultural differences

Diversity data collection – Level setting



Data privacy considerations

- Data privacy considerations
 - Who should be able to review the data
 - How and where the data will be kept / maintained
 - Cross-border transfer restrictions
 - Restrictions on processing the data
 - Retention periods / retention controls, and other protective measures

Diversity data collection – Level setting



US v. OUS generally

- **US**
 - In the US, it is generally lawful for private companies to collect race/ ethnicity, gender, disability and veteran information with the consent of employees
 - Employers may have obligations under federal discrimination law to track and submit to the EEOC or OFCCP demographic workforce data by race/ethnicity and gender
 - In the US, many states have laws that prohibit employers from making any non-job-related inquiry of an employee or applicant that expresses any limitation, specification or discrimination as to a protected category
- **OUS**
 - Outside of the US, restrictions on the type of demographic and diversity data companies can collect from employees are more severe than in the US
 - More companies outside of the US consider voluntary reporting



02 Pay transparency / pay equity reporting requirements

Equal Pay – Why Collect Pay Data

Strategic considerations

The "right" thing to do, and ensuring equal pay can positively impact employee morale, engagement and retention in a competitive landscape for talent

Agency scrutiny – federal and state governmental agencies, including the EEOC, OFCCP, and California CRD, have made pay equity a key focus

Increasing obligations to disclose pay information (e.g., California pay reporting obligations and the potential revival of federal EEO-1 disclosure requirements)

Litigation risk – many companies in the US have faced putative class actions alleging systemic pay discrimination

Individual states are enacting legislation (e.g., California, Massachusetts, New York and New Jersey) that makes it easier to bring equal pay claims and harder to justify pay differences

Increasing prospect of public audits: better to look behind the curtain now



03 Collecting contingent worker ID&E data and tracking supplier diversity

Contingent worker considerations

Considerations when collecting ID&E data from contingent workers

Consider:



Self-identification



Collecting ID&E data
from the staffing agency



If using workers and
collecting data from
multiple staffing
agencies, multiple
sources of
Information may
lead to inconsistency



Collecting data yourself
could lead to
co-employment risks

Tracking supplier diversity



Considerations when tracking supplier diversity

- Metrics to consider:
 - Number of diverse suppliers
 - Percentage of diverse suppliers
 - Tracking diverse supplier spend, and benchmarking industry spend
 - Tier I diverse spend
 - Tier II diverse spend
 - Economic impact
 - Company trends – such as:
 - How metrics changed year over year or quarter over quarter
 - How specific initiatives, marketing campaigns (internal and external), or the implementation of new tools impacts your supplier diversity program
 - How often your supplier diversity program's metrics align with the overall goals of the company



04 Disclosing ID&E data: avoiding pitfalls and setting expectations

Sharing diversity data



Pitfalls of sharing diversity data with employees and shareholders

- Increased litigation / fueling existing litigation
- Improper use, assumptions, and/or conclusions
- Conflicts with EEO-1 disclosure
- Running afoul of data privacy protections (such as the California Consumer Privacy Act, GDPR)
- Requests for additional information
- Possible serious repercussions for employees because of cultural sensitivities

Sharing diversity data



Rules of the road for sharing diversity data

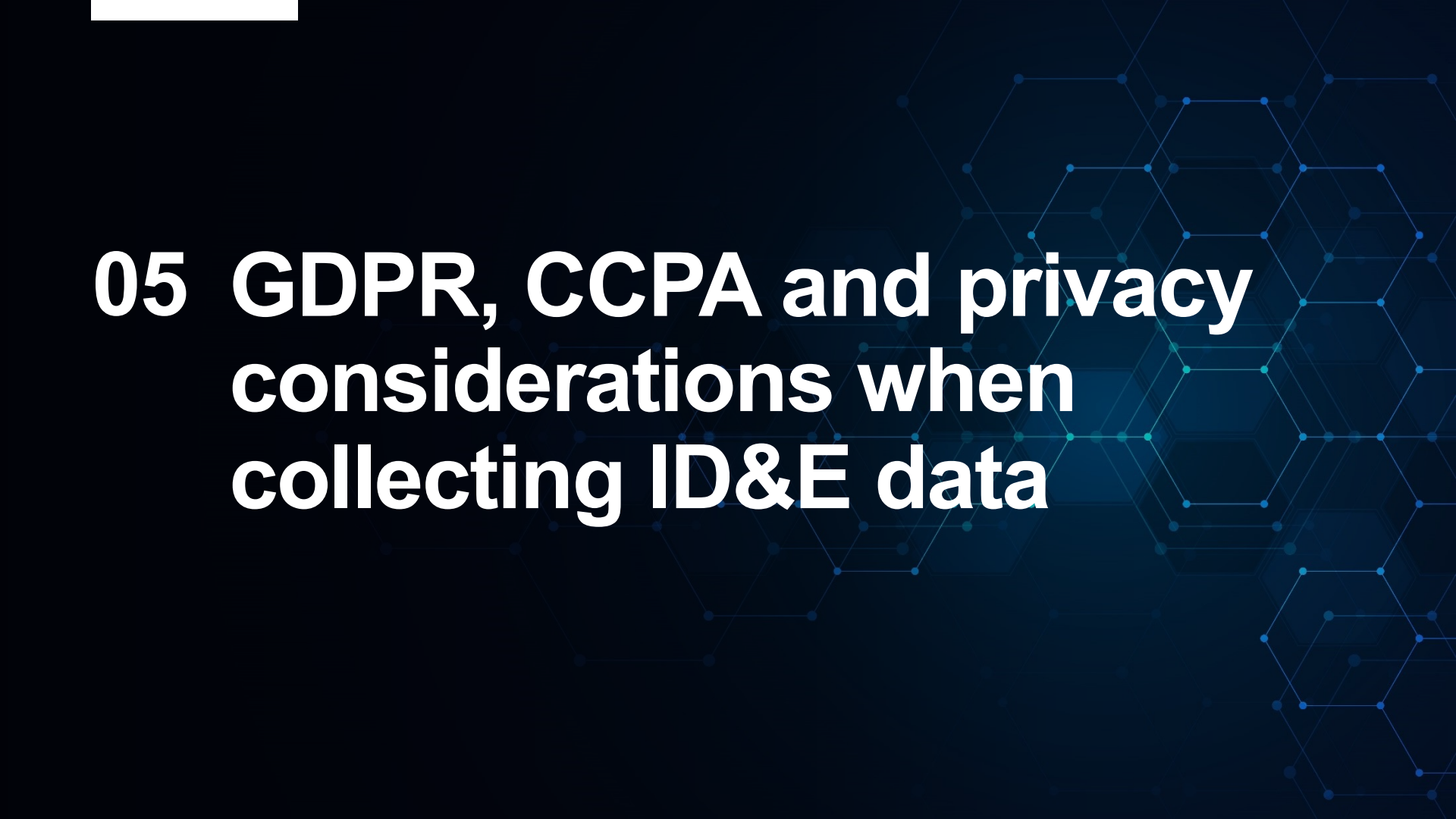
- Develop a cohesive strategy around privilege and confidentiality, ensuring limited access (where practicable) to those with a need to know
- Sufficiently train and communicate with those who have access to the data
- Consider data access and presentation
- Consider employee threshold
- Utilize company teams to balance openness with privacy concerns
- Avoid unnecessary characterizations of diversity-related data
- Avoid quotas, focusing on instead on aspirational goals that are realistic based on data

Sharing diversity data



Considerations for public disclosure of diversity data

- Public disclosure can take many forms. What metrics are most useful to your company?
- Past disclosures are relevant to future disclosures. Ask:
 - What categories of information has the company publicly disclosed in the past?
 - In light of the company's ID&E goals, what story does this data tell?
 - Are there non-quantitative disclosures that would help tell the story?
 - What would be the consequences if the company didn't disclose or modified the categories of disclosure?
- Consider the company's goals.
 - How will / can disclosure help your company's ID&E story?
 - Where will you disclose?
 - Will disclosing steps the company has taken with regard to ID&E be better than just disclosing numbers?
- What is the company doing with its ID&E supplier program?
- Consider who will take note of the disclosure and what they've asked for.



05 **GDPR, CCPA and privacy considerations when collecting ID&E data**

Thinking through privacy considerations

GDPR

- Under Article 9(1) of the General Data Protection Regulation including as currently operative in the U.K. (GDPR), processing special categories of personal data is prohibited unless an exception applies under GDPR Article (9)2.
- Article 9(1) of the GDPR prohibits processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.
- Certain exemptions under GDPR may be applicable for processing of ID&E related data, including
 - (i) with the explicit consent of the employee or applicant
 - (ii) where processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller (i.e., employer) or of the data subject (i.e., employee / applicant) in the field of employment and social security and social protection law
 - (iii) where processing is necessary for reasons of substantial public interest.
 - Nation states in the EU are permitted to impose additional conditions and limitations on the processing of sensitive data. (For example, in Germany, LGBTQ+ data is subject to additional obligations within the employment context, and certain types of sensitive data can be processed only if done so anonymously.)



Thinking through privacy considerations

A word about consent under GDPR

- Consent is rarely considered to be freely given under the GDPR based on the assumption that there is an imbalance of power between employers and employees.
- Consent must be "freely given, specific, informed and unambiguous."
- Consent is not "freely given" where a "clear imbalance of power" between the employer and employee exists.
- Employees can only give free consent in "exceptional circumstances, when it will have no adverse consequences at all whether or not they give consent" and employees must have the right to withdraw consent at any time.
- Article 7 warns against "bundling" consent with standard contract terms.

Thinking through privacy considerations

California Consumer Privacy Act, as amended by the California Privacy Rights Act

- The California Consumer Privacy Act (“CCPA”), as amended by the California Privacy Rights Act (“CPRA”) (collectively, “California Privacy Law”) requires employers to issue privacy notices to their California job applicants, employees, independent contractors and other personnel "at collection," and generally triggers notice requirements for the collection of diversity and inclusion data.
- Effective January 1, 2023:
 - Businesses are required to include in a privacy policy information about their personal information handling practices about California job applicants, employees, independent contractors and other personnel.
 - California residents have the right to request that businesses limit the use of their "sensitive personal information," including information about racial or ethnic origin, to certain business purposes.
 - That said, businesses in California may be able to rely on legal requirements for some processing of ID&E data. For example, private employers with 100 or more employees in California are required to maintain and report employee pay data for specified job categories by gender, race and ethnicity.

Collecting and documenting diversity data




Create an ID&E data protocol with a sound data-retention policy

- Identify the members of your project team, including a well-trained "data protocol officer" who is in charge of properly gathering and using sensitive information
- Clarify who is authorized to analyze the data
- Establish a procedure for adding new members to the team
- Delineate the scope of the team's work
- Clarify that nobody may share sensitive information outside the team without the data protocol officer's approval
- Clarify that violation of the protocol may lead to disciplinary action
- Anyone with access to diversity metrics must be trained to know what is and isn't permitted
- Most companies already have a policy in place regarding how long to keep other kinds of data. If possible, adapt the policy you have in place regarding how long to keep other kinds of data for use with ID&E data
- Make sure that your policy complies with local and other laws
- Follow the general principle that you should retain your data only as long as necessary to identify problems and measure the effectiveness of specific ID&E interventions

06 Appendix





**A. Appendix: Diversity data
collection from a US
and global perspective**

Diversity data collection OUS



A general view of OUS collection

- **EMEA**
 - For some European jurisdictions (i.e., France, Ireland, Spain, UK) collection of diversity data must comply with GDPR and local privacy laws
 - Many jurisdictions (i.e., France, Ireland, Spain, UK) do not permit such collection—usually because the data is deemed sensitive, consent is not a valid basis from a privacy law perspective, and no other legal basis for processing the sensitive personal data is available
 - Broadly speaking, collecting gender (male/female) and veteran status information is not considered to be sensitive / special category information under privacy laws
 - But information about an employee's race/ethnicity, gender identity (which can implicate sexual orientation), sexual orientation and disability status for the purposes of a company's diversity initiative is considered sensitive/special category personal data
 - Where companies do decide to collect this information, only collect it if the diversity data can be anonymized to mitigate privacy risks

Diversity data collection OUS



A general view of OUS collection

- **APAC**
 - Generally allows the collection of ethnicity / race, gender (i.e., gender assigned at birth), gender identity, preferred pronouns, sexual orientation, disability status, and veteran status data, mostly subject to employee consent
 - But the collection of some types of diversity data (e.g., gender identity and sexual orientation) is not recommended from a cultural perspective in certain countries as this may put employees in a vulnerable position and expose them to discrimination or harassment (such as in India and Singapore)
 - In a few jurisdictions, it is required that employers collect and sometimes publicize such data (such as in Australia and Japan)
- **LATAM**
 - Similar to APAC, subject to notice and, in some cases, consent, employers in Latin America are generally permitted to collect personal data
 - And some jurisdictions require collection (such as Brazil, where companies must collect diversity data during onboarding to comply with legal obligations to report that information to the government)



**B. Appendix:
Pay transparency /
pay equity reporting
requirements**

Pay Equity

Approaches to pay transparency

- Growing trend in the US to require the disclosure of pay-related information to employees and applicants. This includes:
 - Affirmative obligations to place pay ranges on job postings;
 - Reactive requirements to disclose pay ranges upon request of employees and applicants;
 - Hybrid requirements to provide pay information both affirmatively and in response to requests.



US Reporting



Heightened obligations for employers to report pay data and maintain records

- **California's** pay data reports must include number of employees by race, ethnicity and sex whose annual W2 earnings fall within each of the pay bands the US Bureau of Labor Statistics uses in the Occupational Employment Statistics survey.
- **New York State's** new salary disclosure law will require employers to maintain a historical record of compensation ranges advertised for jobs, promotions, and transfers.
- In **Illinois**, private employers with 100 or more employees in Illinois who are required to file an annual EEO-1 with the Equal Employment Opportunity Commission (EEOC) are required to provide demographic and wage data.
- Under Colorado's Equal Pay for Equal Work Act, **Colorado** employers must maintain job descriptions and wage-rate history for current employees and, for two years after the employment ends, for former employees.

OUS Reporting



General lay of the land

- **EMEA:** Several jurisdictions have pay gap / pay equity reporting data requirements, including UK, Austria, and countries under the EU Pay Transparency Directive.
- **LATAM:** Though many jurisdictions have laws mandating equal pay for equal work, most countries embrace the International Labor Organization's notion of "work of equal value", and gender discrimination is forbidden in several countries, most jurisdictions do not have reporting requirements.
- **APAC:** Most jurisdictions have the concept of gender pay equity in legislation, though there are still some jurisdictions where there are no comprehensive workplace anti-discrimination laws in place (e.g., Malaysia).
 - Though almost all jurisdictions in APAC don't have a gender pay reporting obligations, there are some that do (such as Australia and Japan).

Resources



Global Data Privacy & Security Handbook

It has never been easier for companies to collect, copy and transfer personal data around the world. But at the same time, the introduction of a wide range of privacy and security laws worldwide imposes complex and often inconsistent privacy and data protection standards impacting multinational companies. Our Global Privacy Handbook provides detailed overviews of the increasingly complex and sophisticated privacy and data protection standards in over 50 countries.



Connect on Tech

Our blog and podcast series covering a broad range of topics such as data privacy and security, cybersecurity, digital innovation and transformation, generative AI and machine learning, and other topics. The podcast features 10-minute interviews with Baker McKenzie attorneys across the globe to discuss practical tips and the impact of data and technology on business.

The image features a large white speech bubble on the left side, set against a dark blue background. The background is decorated with a faint, glowing hexagonal grid pattern of light blue lines and dots. The word "Questions" is written in a bold, black, sans-serif font inside the white bubble.

Questions



Scan QR Code to access
The Employer Report blog`

Baker McKenzie delivers integrated solutions to complex challenges.

Complex business challenges require an integrated response across different markets, sectors and areas of law. Baker McKenzie's client solutions provide seamless advice, underpinned by deep practice and sector expertise, as well as first-rate local market knowledge. Across more than 70 offices globally, Baker McKenzie works alongside our clients to deliver solutions for a connected world.

bakermckenzie.com

Baker & McKenzie LLP is a member firm of Baker & McKenzie International, a global law firm with member law firms around the world. In accordance with the common terminology used in professional service organizations, reference to a "partner" means a person who is a partner, or equivalent, in such a law firm. Similarly, reference to an "office" means an office of any such law firm. This may qualify as "Attorney Advertising" requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.

© 2023 Baker & McKenzie LLP