Photo by Daria Nepriakhina on Unsplash

Many organizations are proactively advancing diversity and inclusion goals globally to include a focus on recruitment and employee-directed initiatives. These efforts are consistent with organizational values and business goals, even in cases where diversity data collection may have the potential to increase (rather than decrease) risks of discrimination claims. Beyond addressing D&I to comply with anti-discrimination laws, most organizations also consider it an urgent business need for commercial success. In moving from actions to outcomes, organizations are seeking to identify and utilize metrics to measure progress, impact and accountability to include the collection of diversity-related data. Privacy and employment law professionals are increasingly being asked to expand such programs globally.

Privacy and employment laws impacting D&I data collection programs and efforts vary greatly, and this is an area undergoing rapid change. No one size fits all, but most multinational organizations should differentiate between their data collection programs at least at a regional level to reduce the risk of their programs being challenged on privacy law grounds. In most cases, the types of information collected for D&I programs are considered sensitive or special categories of personal information and subject to

heightened requirements under privacy laws. And in some jurisdictions, asking about certain traits is prohibited or not recommended because it can cause liability or even safety concerns for the individual and the company.

California

For employers in the United States, the California Consumer Privacy Act, as amended by the California Privacy Rights Act, contains the most prescriptive privacy law requirements. The CCPA currently requires employers to issue privacy notices to their California job applicants, employees, independent contractors and other personnel "at collection," pursuant to a CCPA amendment that took effect on Dec. 16, 2020, which generally triggers notice requirements for the collection of diversity and inclusion data. Such "notices at collection" must include details about the types of personal and sensitive personal information collected from this group, the purposes for which the information is collected, and how long the information is retained or the criteria for determining the same. Effective Jan. 1, 2023, the limited, temporary carve-out for CCPA compliance obligations with respect to personal information from current and potential employees and contractors will expire. Businesses will then be required to include information about their personal information handling practices about this group also in their public-facing online CCPA Privacy Policy.

Also effective Jan. 1, 2023, California residents will have the right to request that businesses stop using their "sensitive personal information," including information about racial or ethnic origin, for purposes outside of various narrow exceptions. These CCPA opt-out rules on sensitive personal information will apply also in the employment context. And to remain compliant with the CCPA, businesses operating D&I data collection programs may be required to offer a way to opt out of the programs via a link on their public-facing website, because the data use may involve inferring characteristics and go beyond the processing of sensitive personal information deemed necessary under the CCPA to perform the services (by employers to employees) reasonably expected by an average consumer who requests such services (one of the exceptions to the opt-out requirement). What an employee may expect of a D&I data collection program may vary by organization and over time. But it is clear that the obligations imposed on businesses by the CCPA shall not restrict a business's ability to comply with the law. And businesses may be able to rely on legal requirements for some processing of D&I data. For example, private employers with 100 or more employees in California are required by California Government Code Section 12999 to maintain and report employee pay data for specified job categories by gender, race and ethnicity. Stay tuned for the delayed CCPA regulations that may shed further light on this use case of

employers processing sensitive personal information as part of D&I data collection programs.

Europe

Before extending a D&I data collection program to countries in the European Economic Area or the U.K., employers should be aware that 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 — including information about racial or ethnic origin and data concerning a natural person's sex life or sexual orientation — is prohibited unless an exception applies under GDPR Article 9(2).

Article 9(2) of the GDPR provides exemptions to the prohibition of processing special categories of personal data, including (i) consent, (ii) where processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or the data subject in the field of employment and social security and social protection law, and (iii) where processing is necessary for reasons of substantial public interest.

Subject to limited exceptions, 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. But increasingly, companies are able to rely on processing being necessary to carry out their legal obligations as more and more European countries require employers to collect and publish diversity data, primarily regarding gender.

For instance, in Italy, according to a law enacted in November 2021, employers with more than 50 employees are required to submit a report every two years outlining certain information, including the number of male and female employees, the number of men and women hired over the reference period, differences in pay, level and role, and specifying for each individual their gender, to assess the equal employment situation of the company. Companies employing up to 50 employees can submit the report voluntarily, suggesting that collecting gender information as part of a D&I program is justifiable in Italy, even for employers with a lower headcount.

Similarly, in Spain, ethnicity data should be considered when preparing "Equality Plans," as long as such data could influence employees' right to equality. Equality Plans contain an ordered set of concrete measures to remove the obstacles that impede or hinder the effective equality of women and men. Since March 7, 2022, Equality Plans have been mandatory for all companies with more than 50 employees. To implement an Equality Plan, companies in Spain must carry out an internal assessment, share the results with employees representatives (and, in their absence, with unions) and negotiate remedial measures. As a result, the ethnicity data as

part of the hiring/onboarding process should also be considered when making the assessment for the Equality Plan.

The GDPR did not fully harmonize privacy laws within this region. Thus, what is considered a special category of personal data also varies within the region, and not all D&I information may be considered a special category of data. For example, gender data is not considered a special category of personal data in France and is not subject to the heightened requirements under GDPR Article 9.

Asia-Pacific

In the Asia-Pacific region, subject to obtaining employee consent (and not subject to the same challenges as in Europe), employers are generally legally permitted to collect D&I data, including ethnicity data, about their workforce for D&I program purposes. In a few jurisdictions, it is required that employers collect and sometimes publicize such data. In Australia, the Workplace Gender Equality Act 2012 requires employers with 100 or more Australian employees to collect gender diversity data (and submit an annual report to the Workplace Gender Equality Agency).

Latin America

Much like the Asia-Pacific region, subject to notice and, in some cases, consent, employers in Latin America are generally permitted to collect personal data for D&I program purposes.

And in certain Latin American jurisdictions, employers are legally required to collect this data. In Brazil, companies must collect diversity data during onboarding to comply with legal obligations to report that information to the government.

Conclusions and outlook

Creating or expanding a global D&I data collection program can be done in a legally compliant way. In order to reduce legal risks both related to discrimination claims and privacy law violations, organizations should carefully consider how to design their D&I data collection and use program, including which categories of data to collect and where. And employers should be aware that expectations about the types of D&I information they should collect may vary. For example, persons in the United Kingdom may increasingly expect race and ethnicity data to be considered in multiple layers, after the U.K. Government Statistical Service started developing a harmonization standard and the United Kingdom 2021 Census collected this information in a layered way. Regional approaches work for some organizations focused on particular D&I data, and more tailored methods are warranted for programs that collect more extensive information in jurisdictions where such collection and processing is permissible. Any D&I data collection program and efforts should include considerations on data storage and access controls, and

organizations must have protocols in place to reduce risks that information is used in a way that could be discriminatory or improper.

While there can be pressure to develop a one-size-fits-all strategy, companies should plan a multifaceted approach for their business that translates locally, aligns with their company culture, and maintains legal compliance with equal opportunity and data privacy laws.

Authors


Loic Coutelier, Nonmember Contributor


Helena Engfeldt, CIPP/E, CIPP/US, IAPP Member Contributor