Published on *The National Law Review* https://natlawreview.com

Workplace Diversity, Equity, Inclusion: Data Privacy and Security Issues

Article By:

Joseph J. Lazzarotti

Kimya S.P. Johnson

Mary T. Costigan

In the last decade, organizations of varied industries and sizes have heightened their focus on diversity, equity, and inclusion (DEI) initiatives and, since 2020, DEI has become a top priority. COVID-19 pandemic realities, racial and social justice movements, changes in federal, state, or local laws, and generational shifts have increasingly brought DEI to the forefront.

Now, more than ever, employees and customers are looking for thoughtful and impactful corporate response. Strong DEI performance is not only a business imperative. DEI is an organizational, leadership, and, increasingly, a legal and compliance imperative.

Many factors have created new risks that could devastate corporate reputations and severely damage brands. Examples include U.S. demographic changes resulting in significantly more diverse workforces, government agencies intensifying antidiscrimination enforcement efforts, and 24-hour global communications. While organizations are investing significant time and resources in enhancing their DEI initiatives, and some are developing comprehensive DEI strategic plans, often overlooked are the data privacy and security considerations involved.

What Personal Data is Collected under the “DEI” Umbrella?

An effective organizational DEI strategy relies on policies and practices that support DEI in all facets of employment, from recruiting and hiring, to onboarding and training, to development and promotion, and, ultimately, to the c-suite and the boardroom. During all phases, a comprehensive DEI strategy contemplates significant collection, use, transfer, and storage of personal information of employees and applicants. This includes data on ethnicity, race, and gender identity, as well as data about sexual orientation, disability, and veteran status, among other key identifiers.

For example, an organization might undergo a diversity assessment. Such an assessment might include, among other things, a legal vulnerability assessments or “diagnostic” assessment that examine internal complaint processes, employment discrimination/retaliation/harassment/hostile work

environment claims, human resource policies and practices and workforce demographic trends.

While a complete discussion of such assessments is beyond the scope of this article, it is important to consider what types of DEI personal data will be collected and from where. Examples of this information may include information related to an employee or applicant's race, gender, sexual orientation, national origin, and disability, among other personal information.

Antidiscrimination Law – DEI Data Collection Requirements

In addition to DEI data that an organization collects for business objectives, U.S. legislation and guidance requires or recommends the collection of certain types of DEI data. Here are just a few examples.

- Employers with 100 or more employees are required to submit an EEO-1 data report to the Equal Employment Opportunity Commission (EEOC) by March 31st of each year, collecting data on race and gender, to help the EEOC identify potential discriminatory employment practices. (The EEOC did not collect employer EEO-1 data in 2020 due to the COVID-19 pandemic.)

- While not required by law, the Uniform Guidelines on Employee Selection Procedures (UGESP) recommend gender and race data collection of applicants to ensure non-discriminatory hiring practices. The UGESP are considered by federal courts when assessing a discriminatory hiring claim under Title VII of the Civil Rights Act.

- The Federal Housing Finance Agency issued AB 2021-01 in March 2021, announcing standards for regulated entities (including federal home loan banks) on data collection relating to the diversity of boards of directors.

- Beginning March 2021, California's SB 973 required covered employers (generally, those with more than 100 employees) to report data relating to employees during a single pay period from the previous calendar year. In addition to annual earnings and hours worked for these employees, reporting must include race, ethnicity, and sex across specified job categories.

Similar obligations and recommendations exist in other parts of the globe. In the European Union (EU), while there is no direct legal duty for diversity reporting, the uniformly worded Article 11(1) of the Racial Equality Directive and Article 13(1) of the Employment Equality Directive put workplace monitoring to foster "equal treatment" first in their list of "exemplary measures," the adoption of which should be considered by employers. They state as follows:

Member States shall, in accordance with national traditions and practice, take adequate measures to promote the social dialogue between the two sides of industry with a view to fostering equal treatment, including through the monitoring of workplace practices, collective agreements, codes of conduct, research or exchange of experiences and good practices.

In addition, in many EU Member States, a special duty has been imposed on employers to collect data on the number of employees with disabilities for the purpose of demonstrating compliance with legally imposed quotas.

Privacy & Security Implications of DEI-Related Data

Privacy (and Data Transfer) Considerations

Privacy. While collection, use, transfer, and storage of personal employee and applicant data are key components of an effective DEI strategy and can be required by national antidiscrimination laws, there are privacy restrictions to consider.

The California Consumer Privacy Act (CCPA) took effect January 1, 2020, imposing a broad range of requirements regarding collection and processing of personal information of California residents. While employee personal information is exempt from most of the CCPA's protections, one relevant area of privacy compliance remains: providing a notice at collection. Covered businesses are required to inform applicants and employees as to the categories of personal information they collect and the purposes for which it will be used. The CCPA was substantially amended in November 2020, when California voters passed California Privacy Rights Act (CPRA), including with respect to the notice-at-collection requirement for employees, job applicants, and independent contractors. The changes become effective January 1, 2023.

First, in addition to the information above, the notice at collection must include information on the retention periods for personal information.

Second, the CPRA expands the existing antidiscrimination rights of consumers to employees, applicants, and independent contractors. Section 1798.125 (a)(1)(E) states:

A business shall not discriminate against a consumer because the consumer exercised any of the consumer's rights … including … retaliating against employee, application for employment, or independent contractor ….

In light of the expansion of this provision, employers now cannot discriminate or retaliate against employees, applicants, and independent contractors exercising their rights to: (i) receive a notice at collection concerning their personal information, and (ii) file a private right to action following a data breach involving their personal information caused by the failure of the employer to maintain reasonable safeguards.

The CPRA also added special protections for DEI data. The definition of personal information has been amended to add "sensitive personal information." This new category includes a "consumer's racial or ethnic origin, religious or philosophical beliefs, or union membership" and "a consumer's sex life or sexual orientation" when used to uniquely identify the consumer. Consumers have the right under these changes to limit the use and disclosure of these and other categories of sensitive personal information.

For organizations operating outside the United States, the privacy implications of a DEI program will be considerably greater. Managing the interplay between federal, state, and local laws, together with laws outside the United States, may require tailoring the DEI program by jurisdiction.

Under the EU's General Data Protection Regulation (GDPR), for example, processing (*e.g.,* collection, storage, and use) personal data is bound by certain requirements and restrictions. The GDPR makes a clear distinction between the processing of personal data and sensitive personal data. Under the GDPR "special categories of data," sensitive personal data is subject to heightened protections and, generally, much of the data collected in a DEI program qualifies as sensitive

personal data.

Art. 9 of the GDPR:

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 shall be prohibited.

The following exemptions under GDPR may be applicable for processing of DEI-related data:

- Art. 9(2)(a) – The explicit consent of the data subject (*i.e.,* employee or applicant).
- Art. 9(2)(b) – Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment.

While consent is considered a legal basis for processing sensitive personal data under the GDPR, EU Data Protection Authorities (DPAs) have stressed that the use of employee consent requires careful evaluation. The GDPR provides that consent must be "freely given, specific, informed and unambiguous." Moreover, the GDPR adds, consent is not "freely given" where a "clear imbalance of power" between the data controller (*i.e.,* employer) and the data subject (*i.e.,* employee) exists. DPAs have questioned the employee's ability to give valid consent because of their dependence on the employer. The inherent imbalance in the employment relationship calls "voluntary" consent into question.

An advisory board comprised of a representative from the DPAs of each EU member state, the European Data Supervisor, and the European Commission, called the Article 29 Working Party, has provided some guidance: "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.

In addition, Article 7 of the GDPR warns against "bundling" consent with standard contract terms. The Working Party advises that Article 7 seeks to ensure the purpose of personal data processing is not disguised or bundled with the provision of a contract of a service for which these personal data are not necessary. Therefore, if an organization is using consent as a legal basis for processing personal data, consent provisions should be in a document separate from the general employee agreement to ensure consent is not associated with the employee's acceptance of employment.

Further, nation states within 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.

In 2016, the European Commission released a revised edition of the European Handbook on Equality and Data to promote equality and contribute to fight discrimination in the EU by analyzing why and what kind of data should be collected in relation to equality and discrimination. Although the Handbook was published before the GDPR took effect, it discusses and takes into consideration GDPR data protection requirements. The Handbook acknowledges the complex interplay between antidiscrimination and data protection legislation, and the challenges in implementing a compliant DEI

program as a result. The Handbook states:

The collection, processing and use of equality data is generally regulated by a combination of antidiscrimination and data protection legislation. As a consequence, there is no coherent approach in relation to the definitions, classification and categorisation of data.

Moreover, the lack of uniform definitions and categories across the EU Member States creates inconsistencies. This is most evident with regard to the grounds of disability and racial/ethnic origin, where the approaches adopted are the most diverse.

Despite the complexities, the Handbook advises that, in the employment context, "diversity monitoring" is not "inherently problematic or challenging" and provides two options and guidance taking into consideration the GDPR, for legal and ethical diversity data collection: (1) collection of personal data associated with identifiable individuals or (2) anonymous workforce surveys.

If collecting personal data of identifiable individuals, the Handbook emphasizes that disclosure of such information *must be voluntary* and provides several best practices:

- Employers should explain clearly the purpose of monitoring (promotion of equal treatment);
- Employers should be able to guarantee the confidentiality of the data;
- Employers should act upon their findings;
- The monitoring form should be carefully designed;
- It should be concise so as not to pose a disproportionate burden;
- The questions should be formulated in clear language; and
- The form should be tested before use.

The Handbook notes that, unsurprisingly, collection of anonymous data has resulted in significantly higher response rates among the equality groups, especially among individuals with disabilities and LGBT+ individuals. Moreover, the Handbook recommends that anonymous data be processed where feasible to reduce the likelihood of misuse and improve voluntary participation. Nonetheless, the collection of anonymous data does not always serve the purpose of the DEI initiative, thus compelling the collection of identifiable individual data.

Data Transfer. In addition to privacy requirements for data processing, employers needing to transfer DEI personal data from European Economic Area (EEA) to the United States (or other countries the European Commission has determined do not have appropriate data protection safeguards) will need to consider how to do so through an adequate transfer mechanism.

Examples of data transfers within a DEI program include accessing a global DEI database from the United States or sending employee data from the EEA to U.S. headquarters. Until recently, many organizations relied on the EU-U.S. Privacy Shield program. However, in July 2020, the Court of Justice of the European Union (CJEU) declared the EU-U.S. Privacy Shield invalid in *Data Protection Commissioner v. Facebook Ireland and Schrems* (C-311/18) (*Schrems II)*.

Alternative methods of transfer include mechanisms such as binding corporate rules (BCRs) for intragroup transfers or standard contractual clauses (SCCs) for intracompany transfers, as well as transfers to third parties. SCCs are clauses approved by the EU as providing reasonable safeguards to data transferred from the EEA. The CJEU did not invalidate either of these transfer mechanisms in *Schrems II,* but it placed SCCs under heightened scrutiny. The CJEU emphasized the data exporter's obligation to verify the data importer's ability to provide EEA data an adequate level of protection. The data exporter must review each transfer to determine on a case-by-case basis whether the SCCs provide sufficient reasonable safeguards, particularly in light of the recipient country's surveillance laws. As a result, data exporters must review applicable local legislation for each transfer to identify when SCCs are adequate, whether supplemental protective measures are required, or whether the transfer cannot occur. A comparable analysis will apply to BCRs. On June 4, 2021, the EU Commission adopted long-awaited updated SCCs (replacing 2001, 2003, and 2010). The updated SCCs address more complex processing activities, the requirements of the GDPR, and the *Schrems II* decision. These clauses are modular so they can be tailored to the type of transfer.

Businesses seeking to find an alternative to the EU-U.S. Privacy Shield, BCRs, or SCCs should review whether a transfer may fall under one of several exceptions to the GDPR's requirement of an adequate transfer mechanism. Many of these exceptions, however, apply only when the transfer is necessary, occasional, and affects a limited number of data subjects.

Under the GDPR, impermissible processing or transfer can result in assessment of fines up to €20 million or, in the case of an undertaking, up to four percent of the total worldwide annual turnover of the preceding financial year, whichever is higher. In addition, EU data subjects may bring a private cause of action against the data exporter for an illegal transfer, either individually or as part of a class action.

Security Considerations

With data security incidents (*e.g.,* mass data breaches and phishing scams of employee personal) on the rise in recent years, implementing reasonable security safeguards has never been more important. In response to such incidents, data security legislation continues to expand in the United States and abroad. However, in the United States, the laws requiring data security measures to protect personal information and notification in case of a breach typically extend to a narrow set of personal information that typically does not include traditional DEI data. Nonetheless, because of compelling privacy concerns relating to such data, along with the more expansive view of privacy and security in the EU and other jurisdictions, extending data security measures to include DEI data is prudent and may be mandatory.

The CCPA (discussed above in the privacy context) permits employees to commence a private right of action if affected by a data breach involving personal information caused by a failure of the employer to maintain reasonable safeguards. Effective in 2020, New York's Stop Hacks and Improve Electronic Data Security Act (SHIELD Act) requires any business that owns or licenses the private information of New York residents to develop, implement, and maintain reasonable safeguards to protect the security, confidentiality, and integrity of the private information. These provisions do not apply to DEI data.

Still, there is good reasons to include DEI under the umbrella of an organization's written information security program. Employees may be more likely to participate if they believe the company takes the security of their personal information seriously. A breach of such data could create unintended consequences, especially for organizations still developing their DEI programs.

Many organizations rely on consultants and other service providers to assist them with DEI program development, reporting, and consulting. Therefore, these services providers may store significant amounts of employee personal information, including DEI data. In this case, organizations should also assess the practices of those service providers and obtaining their written assurances to safeguard that data. For example, even if HR outsources certain processes involving DEI data to third-party vendors, it should ensure those vendors have reasonable safeguards in place.

For organizations that operate outside the United States, there are additional security obligations for protection of personal data to consider. Under the GDPR, for example, an organization that processes personal data “shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.”

While this rapidly developing area of the law presents compliance challenges, legislation generally does not mandate specific safeguards. Rather, legislation provides examples of practices that are considered reasonable administrative, technical, and physical safeguards based on the size and scope of the business. For example, practices considered reasonable administrative safeguards include risk assessments, employee training, selecting vendors capable of maintaining appropriate safeguards and implementing contractual obligations for those vendors, and disposal of private information within a reasonable time.

In the development of a DEI strategy, it is important for an organization to take stock of the DEI-related personal data being processed and where it is located and ensure there are reasonable safeguards in place to protect that data.

Key Issues

The balance between antidiscrimination laws and data privacy and security laws, and cultural considerations, is complex, requiring thoughtful planning.

Leadership & Goals:

- Who are the key individuals involved in developing, implementing, and maintaining the DEI program?
    - Executives, HR departments, diversity leadership groups, legal, and IT are all potential stakeholders in a DEI program that may come with different agendas and priorities in mind. For example, an HR recruiting team may aim to capture as much data as possible, while the legal and IT teams may push for more limited collection. It will be important to define roles and responsibilities of those involved, early on.
- What are the goals of the DEI program, initiative, or strategy?
    - The goals will significantly impact that type of data collected. Examples of common goals include increased productivity/creativity/decision-making, a larger job applicant pool, global impact, enhanced corporate reputation, ethical duty, prevention of legal liability, and development, inclusion, or retention of historically underrepresented populations.

DEI Data:

- What data is being collected?
- Who will be responsible for collecting, using, transferring, storing and disposing of the data?
- Who will have access to the data?
- Is it mandatory or recommended by law/guidance to collect such data, as opposed to exclusively a business strategy?
- What is the legal basis for data processing? If consent is needed, how is the consent process facilitated? Who is responsible for the handling the consent process? Do the disclosures or consents mention DEI-related purposes? What if an employee/applicant refuses to consent? Can consent be revoked later?
- Will the type of data change over time? Has the organization already been collecting this data for other business purposes?
- For global organizations, will the type of data collected vary by location?
- Does the organization have a privacy policy related to employee and job applicant personal data already in place? If so, how should it address DEI uses?

Best Practices

The development and implementation of a DEI program will vary greatly depending on the size, location, and goals of the organization. However, best practices for handling DEI data can be applied fairly universally.

- *Culture and location.* The cultural expectations and legal obligations regarding DEI data processing will vary significantly by location. In addition to antidiscrimination and data privacy and security laws, there may be other labor laws or social security laws that require or limit DEI data processing to consider. In addition to legal counsel, the DEI leadership team should maintain a keen awareness of relevant legislation and a general sense of where the law and culture is headed. Further, any DEI leadership team should always consider whether the audience (*e.g.,* employees and customers) are primed to provide their data. A key consideration for any DEI-related data effort is determining whether there has been sufficient training, dialogue, or communication around what data is being sought and why it is being sought – to promote trust and respect throughout the process and maximize participation.

- *Less is more.* As with most forms of data collection within an organization, less often is more. Some organizations pride themselves on their comprehensive recordkeeping systems, for example, claiming to have retained all records since inception. Such practices may not be necessary and, in many cases, are not prudent. Retaining massive amounts of data may be needed in certain contexts, but it should be carried out strategically and deliberately, with a plan to shed the data once its usefulness has ceased.

- *Notice and consent.* As a starting point (to help ensure employee support for the DEI program and prevent legal liability), employees and job applicants should be provided clear notice of the categories of data collected and how the organization will use that data. If consent is the legal basis for collecting data, employees and applicants should be aware of this right, as well the process for how to consent and how to revoke consent if they choose. To ensure consent is not associated with the employee's acceptance of employment, consent provisions should not be bundled with an employee handbook or general employment agreement.

- *Written policies.* Development and implementation of the DEI program should be in writing, and relevant personnel should be trained in its execution. Regarding data privacy and security, there should be a Written Information Security Program, including a risk assessment, in place for how all personal data is being handled within the organization, including DEI-related data. It is not enough to say, "We are doing that." From a compliance perspective, data privacy and security policies and procedures need to be in writing. Additionally, written policies and procedures help to maintain consistency in the organization's practices and better support discipline for violations of the rules.

- *Be reasonable.* Importantly, the steps taken should be reasonable. Indeed, most regulatory data privacy and security frameworks require "reasonable" safeguards. Of course, this is not easy to define, but reasonableness should be a fundamental principle guiding your program.

Takeaway

An effective DEI program protects the organization's reputation and expands business opportunities by strengthening relationships with stockholders, customers, employees, regulators, and the general public. In the tumultuous times of 2020s, DEI initiatives have never been more important for organizational wellbeing. The interplay between privacy and antidiscrimination laws requires a comprehensive understanding of the issues and finding the right balance for the organization.

National Law Review, Volumess XII, Number 29