Workplace Discrimination and Equal Opportunity

Why monitoring cultural diversity in your European workforce is not at odds with GDPR

Prof. Lokke Moerel*

It has been said that figures rule the world. Maybe. But I am sure that figures show us whether it is being ruled well or badly.

Johann Wolfgang von Goethe

1. Introduction

It is a known fact that discrimination persists in today's labor markets,[1] this despite EU anti-discrimination and equality laws—such as the Racial Equality Directive—specifically prohibiting practices that put employees at a particular disadvantage based on racial or ethnic origin.[2] In a market where there is an acute scarcity of talent,[3] we see HR departments struggle with how to eliminate workplace discrimination and create an inclusive culture in order to be able to recruit and support an increasingly diverse workforce. By now, many organizations have adopted policies

* Lokke Moerel is Professor of Global ICT Law at Tilburg University and Senior of Counsel at Morrison & Foerster in Brussels. Ms. Moerel thanks Annabel Gillham, a partner at Morrison & Foerster in London, for her valuable input on a previous version of this article.

[1] For recent statistics, see "A Union of equality: EU anti-racism action plan 2020-2025," https://ec.europa.eu/info/sites/default/files/a_union_of_equality_eu_action_plan_against_racism_2020_-2025_en.pdf, p. 2, referring to wide range of surveys conducted by the EU Agency for Fundamental Rights (**FRA**) pointing to high levels of discrimination in the EU, with the highest level in the labor market (29%), both in respect of looking for work but also at work.

[2] See, specifically, Council Directive 2000/43/EC of June 29, 2000, implementing the principle of equal treatment between persons irrespective of racial or ethnic origin ("**Racial Equality Directive**"), *Official Journal L* 180, 19/07/2000 P. 0022–0026. Action to combat discrimination and other types of intolerance at the European level rests on an established EU legal framework, based on a number of provisions of the European Treaties (Articles 2 and 9 of the Treaty on European Union (**TEU**), Articles 19 and 67(3) of the Treaty on the Functioning of the European Union (**TFEU**), and the general principles of non-discrimination and equality, also reaffirmed in the EU Charter of Fundamental Rights (in particular, Articles 20 and 21).

[3] WEF, Jobs of Tomorrow, Mapping Opportunity in the New Economy, Jan. 2020 ("**WEF Report**"), WEF_Jobs_of_Tomorrow_2020.pdf (weforum.org). See also https://www.mckinsey.com/featured-insights/future-of-work/ai-automation-and-the-future-of-work-ten-things-to-solve-for. There is a shortage of talent that is especially acute in knowledge industries, such as the financial and business services industries where a shortage of 10.7 million candidates is expected by 2030, which will continue to fuel this upward trend in global talent interconnectedness.

to promote *diversity, equity, and inclusion* (**DEI)** in their organizations and the need has arisen to monitor and evaluate their DEI efforts.

Without proper monitoring, DEI efforts may well be meaningless or even counterproductive.[4] To take a simple example, informal mentoring is known to be an important factor for internal promotions, and informal mentoring is less available for women and minorities.[5] Organizations setting up a formal internal mentoring program to address this imbalance would like to monitor whether the program is attracting minorities to participate in the program and achieving its goal of promoting equity. If not, the program may unintentionally only exacerbate existing inequalities. Monitoring is therefore required to evaluate whether the mentoring indeed results in more equal promotions across the workforce or whether changes to the program should be made.

Organizations are hesitant to monitor these policies in the EU based on a seemingly persistent myth that the EU General Data Protection Regulation 2016/679 (**GDPR**) would prohibit such practices. This article shows that it is actually the other way around. Where discrimination, lack of equal opportunity, or pay inequity at the workplace is pervasive, monitoring of DEI data is a prerequisite for employers to be able to comply with employee anti-discrimination and equality laws, and to defend themselves appropriately against any claims.[6]

> The crucial question corporate leaders have to ask is this: Do we really want to wait until *after* we've been sued to learn that our DEI record is problematic?
>
> ***Harvard Business Review*, July 2022**

For historic reasons,[7] the collection of racial or ethnic data is considered particularly sensitive in many EU member states. EU privacy laws provide for a special regime to collect sensitive data categories such as data revealing racial or ethnic origin, disability, and religion, based on the underlying assumption that collecting and processing such data increases the risk of discrimination.

---

[4] For a list of examples why diversity policies may fail: https://hbr.org/2016/07/why-diversity-programs-fail. See also Data-Driven Diversity (hbr.org): "According to Harvard Kennedy School's Iris Bohnet, U.S. companies spend roughly $8 billion a year on DEI training—but accomplish remarkably little. This isn't a new phenomenon: An influential study conducted back in 2006 by Alexandra Kalev, Frank Dobbin, and Erin Kelly found that many diversity-education programs led to little or no increase in the representation of women and minorities in management."

[5] While white men tend to find mentors on their own, women and minorities more often need help from formal programs. Introduction of formal mentoring shows real results: https://hbr.org/2016/07/why-diversity-programs-fail.

[6] Quote is from https://hbr.org/2022/03/data-driven-diversity.

[7] Historically, there have been cases of misuse of data collected by National Statistical Offices (and others), with extremely detrimental human rights impacts, see Luebke, D. & Milton, S. 1994, "Locating the Victim: An Overview of Census-Taking, Tabulation Technology, and Persecution in Nazi Germany." IEEE Annals of the History of Computing, Vol. 16 (3). See also W. Seltzer and M. Anderson, "The dark side of numbers: the role of population data systems in human rights abuses," Social Research, Vol. 68, No. 2 (summer 2001), the authors report that during the Second World War, several European countries, including France, Germany, the Netherlands, Norway, Poland, and Romania, abused population registration systems to aid Nazi persecution of Jews, Gypsies, and other population groups. The Jewish population suffered a death rate of 73 percent in the Netherlands. In the United States, misuse of population data on Native Americans and Japanese Americans in the Second World War is well documented. In the Soviet Union, micro data (including specific names and addresses) were used to target minority populations for forced migration and other human rights abuses. In Rwanda, categories of Hutu and Tutsi tribes introduced in the registration system by the Belgian colonial administration in the 1930s were used to plan and assist in mass killings in 1994.

However, where racial or ethnic background are 'visible' as a matter of fact to recruiters and managers alike, individuals from minority groups may be discriminated against *without* recording any data. It is therefore *only by* recording the data that potential existing discrimination may be revealed, and bias can be eliminated from existing practices.[8]

> Racial origin, like gender, is a matter of fact…. Ethnic records should therefore be seen as an essential tool in achieving racial equality, because without them, it would be difficult to establish the nature or extent of inequality, the areas where action is most needed, and whether measures aimed at reducing inequality are succeeding.
>
> **The UK Commission for Racial Equality, 2000**

Unsurprisingly, minority interest groups that represent the groups whose privacy is actually at stake, actively advocate for such collection of data and monitoring. Equally, EU and international institutions unequivocally consider collection of DEI data indispensable for monitoring and reporting purposes in order to fight discrimination. EU institutions further explicitly confirm that the GDPR should not be considered an obstacle preventing the collection of DEI data, but instead establishes conditions under which collecting and processing of such data are allowed.

From 2024 onwards, large companies in the EU will be subject to mandatory disclosure requirements for compliance with environmental, social, and governance (**ESG**) standards under the upcoming EU Corporate Sustainability Reporting Directive (**CSRD**). The CSRD requires companies to report on actual or potential adverse impacts on their workforce with regard to equal treatment and opportunities, which are difficult to measure without collecting and monitoring DEI data.

Currently, the regulation of collection and processing of DEI data is mainly left to the Member States. EU anti-discrimination and equality laws do not impose an obligation on organizations to collect DEI data for monitoring purposes, but neither do they prohibit collecting such data. In the absence of a specific requirement or prohibition, the processing of DEI data is regulated by the GDPR. The GDPR provides for ample discretionary powers for the Member States to provide for legal bases in their national laws to process DEI data for monitoring purposes. In practice, most Member States, however, have **not** used the opportunity under the GDPR to provide for a specific legal basis in their national laws for processing racial or ethnic data for monitoring purposes (with notable exceptions).[9] As a consequence, collection and processing of DEI data for monitoring purposes is taking place on a voluntary basis, whereby employees are asked to fill out surveys based on self-identification. This is in line with the GDPR, which provides for a general exception allowing organizations to process DEI data based on the explicit consent of the individuals

[8] The quote is from the Commission for Racial Equality (2000), Why Keep Ethnic Records? Questions and answers for employers and employees (London, Commission for Racial Equality).

[9] A notable exception is the UK, which long before its exit from the EU, legislated for the collection of racial and ethnic data to meet the requirements of *the substantial public interest* condition for purposes of both "Equality of opportunity or treatment" and "Racial and ethnic diversity at senior levels" and further provided for criteria for processing ethnic data for *statistical purposes*, *see* Schedule 1 to the UK Data Protection Act 2018 (inherited from its predecessor, the Data Protection Act 1998), and the Information Commissioner's Office Guidance on special category data, 2018. Schedule 1 also provides for specific criteria to meet the requirements of the statistical purposes condition. See https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/.
Another exception is the Netherlands, which allows for limited processing of racial and ethnic data (limited to country of birth and parents' or grandparents' countries of birth) for reason of *substantial public interest.*

concerned, *provided that the Member States have not excluded this option in their national laws*. In practice, Member States have **not** used this discretionary power; they have not excluded the possibility of relying on explicit consent for the collection of DEI data. This leaves explicit consent as a valid, but also the only practically viable, option to collect DEI data for monitoring purposes.[10] Both human rights frameworks and the GDPR itself facilitate such monitoring, provided there are safeguards to protect abuse of the relevant data in accordance with data minimization and *privacy-by-design* requirements.[11] We now see best practices developing as to how to monitor DEI data while limiting the impact on the privacy of employees, and rightfully so. In literature, collecting racial or ethnic data for monitoring is rightfully described as "a problematic necessity, a process that itself needs constant monitoring."[12]

2. The fallacy that "not knowing" leads to more fairness

Data protection laws are based on the underlying assumption that collecting and processing sensitive data elements such as data revealing racial and ethnic origins increase the risk of discrimination. As set out above in the introduction, in the case of "visible" minorities, the relevant data is available as a matter of fact. It is easily (but not always accurately) inferred. Individuals from minority groups may therefore be discriminated against *without* recording any data. It is *only by* recording the data that potential existing discrimination may be revealed, and bias can be eliminated from existing practices.

"Unawareness does not equal fairness"

The magical thinking that dictates that "not knowing" leads to more fairness persists in other areas.[13] For example, in the Netherlands, there is a taboo against "ethnic registration" in connection with crime because it could lead to political abuse. This is a fallacy. Dutch scientists rightly advocated breaking this taboo: "You can only do something about inequality if you first map whether it takes place."[14] As an example, the scientists cited that young people of Moroccan origin rarely show up at a certain governmental agency that is mandated to consider alternative rehabilitation measures for crimes as an alternative to a criminal record. The condition is that these youngsters plead guilty and repent. Doing so is difficult,

[10] For example, in the Netherlands, it is generally accepted that collecting DEI data can take place on a voluntary basis. See Dutch Social Economic Council,"Meten is Weten, zicht op effecten van diversiteits- en inclusiebeleid," Charter Document, pp. 7–10, Dec. 2021. See also the report titled "Het moet wel werken," p. 30, https://goldschmeding.foundation/wp-content/uploads/Rapport-Het-Moet-Wel-Werken-Vergelijkende-analyse-juli-2021.pdf.

[11] The European Handbook on Equality Data (2016) provides a comprehensive overview of how equality data can be collected, https://op.europa.eu/en/publication-detail/-/publication/cd5d60a3-094d-11e7-8a35-01aa75ed71a1/language-en; EU High Level Group on Non-discrimination Equality and Diversity, "Guidelines on improving the collection and use of equality data," 2021, https://commission.europa.eu/system/files/2022-02/guidance_note_on_the_collection_and_use_of_equality_data_based_on_racial_or_ethnic_origin_final.pdf. See also the reports listed in the previous endnote.

[12] Bonnett and Carrington 2000, p. 488.

[13] This paragraph (including the quote) draws on my earlier article published in the *Dutch Financial Times*, and an Op-ed for IAPP, see L. Moerel, "Algorithms can reduce discrimination, but only with proper data," Op-ed IAPP Privacy Perspectives, Nov. 16, 2018, https://iapp.org/news/a/algorithms-can-reduce-discrimination-but-only-with-proper-data/.

[14] https://www.volkskrant.nl/nieuws-achtergrond/onderzoekers-politie-en-justitie-moeten-etniciteit-registreren-van-elke-arrestant-verdachte-en-veroordeelde~bf2f5fcf/?utm_campaign=shared_earned&utm_medium=social&utm_source=email.

however, because of the so-called "shame" culture in Moroccan society. How can we expect to improve this situation if we do not know that it is precisely these young people who stay away? In this case, the potential risk of political abuse is outweighed by the many benefits of mapping these correlations. Again, it is not the *recording* of the sensitive data that is wrong, it is humans who discriminate, and the recording of the data *detects* this bias.

This issue has very much come to the fore where tools are used which are powered by artificial intelligence (**AI**). We often see in the news that the deployment of algorithms leads to discriminatory outcomes.[15] If self-learning algorithms discriminate, it is not because there is an error in the algorithm, it is because the data used to train the algorithm are "biased." It is only when you know which individuals belong to vulnerable groups that bias in the data can be made transparent and algorithms trained properly.[16] That sensitive data may be legitimately collected for these purposes under European data protection law[17] is explicitly provided for in the proposed AI Act.[18]

Example – Discrimination by AI tools

In the United States, "crime prediction tools" were proven to be discriminatory against ethnic minorities.[19] The police stopped and searched more ethnic minorities and as a result this group also showed more convictions. If you use this data to train an algorithm, the algorithm will allocate a higher risk score to this group. Discrimination by algorithms is therefore a reflection of discrimination that is already taking place "on the ground".

As algorithms are always trained on historical data, it is virtually impossible to find a "clean" dataset on which an algorithm can be trained to be "bias-free." To solve this, group indicators such as race, gender, and religion are often removed from the training data. The idea is that if the algorithm cannot "see" these elements, the outcome will not be discriminatory. The algorithm is thus "blinded," just as résumés are sometimes blindly

---

[15] In the U.S., for example, "crime prediction tools" proved to discriminate against ethnic minorities. The police stopped and searched more ethnic minorities, and as a result this group also showed more convictions. If you use this data to train an algorithm, the algorithm will allocate a higher risk score to this group. Discrimination by algorithms is therefore a reflection of discrimination already taking place "on the ground". https://www.cnsnews.com/news/article/barbara-hollingsworth/coalition-predictive-policing-supercharges-discrimination.

[16] See L. Moerel, "Algorithms can reduce discrimination, but only with proper data," Op-ed IAPP Privacy Perspectives, Nov. 16, 2018, https://iapp.org/news/a/algorithms-can-reduce-discrimination-but-only-with-proper-data/.

[17] See also the guidance of the UK Information Commissioner (ICO) on AI and data protection, Guidance on AI and data protection | ICO. In earlier publications, I have argued that the specific regime for processing sensitive data under the GDPR is no longer meaningful. Increasingly, it is becoming more and more unclear whether specific data elements are sensitive. Rather, the focus should be on whether the *use* of such data is sensitive. Processing of racial and ethnic data to eliminate discrimination in the workplace is an example of non-sensitive use, provided that strict technical and organizational measures are implemented to ensure that the data are not used for other purposes. See https://iapp.org/news/a/gdpr-conundrums-processing-special-categories-of-data/ and https://iapp.org/news/a/11-drafting-flaws-for-the-ec-to-address-in-its-upcoming-gdpr-review/.

[18] Article 10(2) sub. 5 of the draft AI Act allows for the collection of special categories of data for purposes of bias monitoring, provided that appropriate safeguards are in place, such as pseudonymization.

[19] https://www.technologyreview.com/2020/07/17/1005396/predictive-policing-algorithms-racist-dismantled-machine-learning-bias-criminal-justice/.

assessed by recruiters,[20] or orchestra auditions are conducted behind a screen, which indeed results in the selection of more female musicians.[21]

In practice, "blinding" does not work for algorithms. "Blind" training does not promote equality or fairness. For example, in the Netherlands, more than 87% of all primary school teachers are female.[22] An algorithm trained to select the best candidates for this job would be fed with the résumés received in the past. Because primary schools employ so many more women than men, the algorithm would quickly develop a preference for female candidates, and making the résumés gender-neutral will not solve this issue. The algorithm would quickly detect other ways to explain why female résumés are selected more often, including by preferring predominantly female hobbies and allocating fewer points to résumés listing traditionally male pastimes.[23]

The lesson is that removing group indicators does not help if the underlying data is one-sided. The algorithm will soon find derived indicators—*proxies*—to explain this bias. The only solution is to first make biases transparent in the training data. This requires that group indicators must be collected first, in order to assess whether minority groups are treated unequally. Then the algorithm must be trained against selecting these factors, by means of "adversarial training."[24] That is the only way to prevent past biases from influencing future outcomes. Companies deploying AI should also be aware that the "fairness" principle under the GDPR cannot be achieved by unawareness. In other words, ***race blind*** is not ***race neutral***, and in the AI context ***unawareness*** does not equal ***fairness***.

3. Towards a positive duty to monitor for workplace discrimination

Where discrimination in the workplace is pervasive, monitoring of DEI data for quantifying discrimination in those workplaces is essential for employers to be able to comply with anti-discrimination and equality laws. As indicated above, there is no general requirement under the Racial Equality Directive to collect, analyze, and use DEI data. This Directive, however, does provide for a shift in the burden of proof.[25] Where a complainant establishes facts from which a *prima facie* case of discrimination can be presumed, it will fall to the employer to prove that there has been no breach of the principle of equal treatment. Where workplace discrimination is pervasive, a prima facie case will be easy to make, and it will fall to the employer to disprove any such claim, which will be difficult without any data collection and monitoring. The argument that the GDPR does not allow for processing such data will not relieve the employer of its

[20] See Aslund and Skans, 2012; Krause *et al.*, 2012 for research on masking of identifying characteristics in resumes. The research on the effectiveness of this approach is mixed. Luc Behaghel, Bruno Crépon, and Thomas Le Barbanchon, "Unintended Effects of Anonymous Resumes," The Institute for the Study of Labor (**IZA**), Discussion Paper No. 8517, Sept. 2014, http://ftp.iza.org/dp8517.pdf, p. 2. In addition, "race-blind" screening processes are not necessarily "race-neutral." If there is a correlation between minority status and other elements in a resume, it may not be difficult for recruiters to reconstruct missing information and continue to discriminate. See, for example, Persico (2009). Similarly, Autor and Scarborough (2008) studied the conditions under which "race-blind" job testing is not necessarily "race-neutral."

[21] Goldin and Rouse (2000) famously showed that American orchestras conducting blind auditions hired more women.

[22] https://www.voion.nl/media/4089/trendrapportage-arbeidsmarkt-leraren-po-vo-en-mbo-2021.pdf.

[23] See n. 15.

[24] See Zhao, W.; Alwidian, S.; Mahmoud, Q.H., Adversarial Training Methods for Deep Learning: A Systematic Review, Algorithms 2022, 15, 283, https://doi.org/10.3390/a15080283.

[25] Article 8 Racial Equality Directive.

burden of proof. *See*, in a similar vein, *European Committee of Social Rights, European Roma Rights Centre v. Greece*[26]:

> **Data collection**
> 27. The Committee notes that, in connection with its wish to assess the allegation of the discrimination against Roma made by the complainant organisation, the Government stated until recently that it was unable to provide any estimate whatsoever of the size of the groups concerned. To justify its position, it refers to legal and more specifically constitutional obstacles. The Committee considers that when the collection and storage of personal data [are] prevented for such reasons, but it is also generally acknowledged that a particular group is or could be discriminated against, the authorities have the responsibility for finding alternative means of assessing the extent of the problem and progress towards resolving it that are not subject to such constitutional restrictions."

As early as 2000, the UK Commission for Racial Equality provided the following official justification for monitoring of ethnic/racial data:[27]

> Although ethnic records are not obligatory under the Race Relations Act of 1976, the legislation does place the responsibility for providing equality of opportunity for all job applicants and employees primarily with employers. Ethnic records are an important tool in fulfilling this responsibility […] the analysis of ethnic data helps not only in identifying and dealing with unlawful discrimination, but also frequently highlights other employment practices in need of improvement.

In addition, as part of the UK's mandatory pre-employment tribunal conciliation process, employees can ask questions of the employer about the discrimination complained of, including statistics about the ethnic make-up of the workforce.[28] This is designed precisely to address the evidential imbalance where the employer holds most of the information proving or disproving the allegations which can prevent an employee from showing facts from which discrimination can be presumed.

In a similar vein, in December 2021, the Dutch Social Economic Council in its Charter Document,[29] indicated that employers can collect special categories of data such as ethnic data, in order to comply with the General Act on Equal Treatment (*Algemene Wet Gelijke Behandeling*

---

[26] Complaint No. 15/2003, decision on the merits, Dec. 8, 2004, § 27.

[27] Commission for Racial Equality (2000) Why keep Ethnic Records? Questions and answers for employers and employees (London, Commission for Racial Equality, as quoted in Bonnett, A., & Carrington, B. (2000)). Fitting into categories or falling between them? Rethinking ethnic classification, *British Journal of Sociology of Education*, 21(4), p. 488. The Racial Relations Act is now replaced by the Equality Act 2010, and the UK Commission for Racial Equality by the UK Equality and Human Rights Commission (**EHRC**). The EHRC has also confirmed that employers can carry out equality-related monitoring to help assess their equal opportunity practices, including by monitoring how many people with a particular protected characteristic apply for each job, are shortlisted and are recruited or promoted. See Good equality practice for employers: equality policies, equality training and monitoring | Equality and Human Rights Commission (equalityhumanrights.com), p. 15.

[28] See "Asking your employer questions about discrimination: Asking and answering questions about discrimination at work" at https://www.acas.org.uk/asking-and-answering-questions-about-discrimination

[29] Dutch Social Economic Council, "Meten is Weten, zicht op effecten van diversiteits- en inclusiebeleid," Charter Document, p. 10, Dec. 2021, https://www.ser.nl/nl/Publicaties/charterdocument-meten-is-weten.

(**AWGB**)), which prohibits employers from, directly or indirectly, treating employees differently in their employment conditions on the basis of, among other factors, race, nationality, or religion.

Since as early as 1989,[30] all relevant EU and international institutions have, with increasing urgency, issued statements that the collection of DEI data for monitoring and reporting purposes is indispensable to the fight against discrimination.[31] See, for example, the EU Anti-racism Action Plan 2020–2025[32] (the "**Action Plan**") in which the European Commission explicitly states:

> Accurate and comparable data is essential in enabling policy-makers and the public to assess the scale and nature of discrimination suffered and for designing, adapting, monitoring and evaluating policies. This requires disaggregating data by ethnic or racial origin.[33]

In the Action Plan, the European Commission notes that equality data remains scarce, "with some member states collecting such data *while others consciously avoid this approach*." The Action Plan subsequently provides significant steps to ensure collection of reliable and comparable equality data at the European and national level.[34]

[30] See, e.g., ECRI General Policy Recommendation No. 4 on national surveys on the experience and perception of discrimination and racism from the point of view of potential victims, adopted on Mar. 6, 1998.

[31] See the Report prepared for the European Commission, "Analysis and comparative review of equality data collection practices in the European Union Data collection in the field of ethnicity," 2017, data_collection_in_the_field_of_ethnicity.pdf (europa.eu), https://op.europa.eu/en/publication-detail/-/publication/cd5d60a3-094d-11e7-8a35-01aa75ed71a1#:~:text=The%20European%20Handbook%20on%20Equality,to%20achieve%20progress%20towards%20equality. For example, the European Handbook on Equality Data initially dating from 2007, already stated that "Monitoring is perhaps the most effective measure an organisation can take to ensure it is in compliance with the equality laws." The handbook was updated in 2016 and provides a comprehensive overview of how equality data can be collected, https://op.europa.eu/en/publication-detail/-/publication/cd5d60a3-094d-11e7-8a35-01aa75ed71a1/language-en.

[32] EU Anti-racism Action Plan 2020–2025, p. 15.

[33] See a longer but similar statement in the 2021 Report of the European Commission evaluating the Racial Equality Directive, p. 14, https://ec.europa.eu/info/sites/default/files/report_on_the_application_of_the_racial_equality_directive_and_the_employment_equality_directive_en.pdf.

[34] EU Anti-racism Action Plan 2020-2025, p. 21, under reference to: Niall Crowley, Making Europe more Equal: A Legal Duty? https://www.archive.equineteurope.org/IMG/pdf/positiveequality_duties-finalweb.pdf, which reports on the Member States that already provide for such positive statutory duty. See p. 16 for an overview of explicit preventive duties requiring organizations to take unspecified measures to prevent discrimination, shifting responsibility to act from those experiencing discrimination to employers. They can stimulate the introduction of new organizational policies, procedures and practices on such issues.

On the international level, the United Nations (**UN**) takes an even stronger approach, considering collection of DEI data that allow for disaggregation for different population groups to be part of governments' human rights obligations. See the UN 2018 report, "A Human Rights-based approach to data, leaving nobody behind in the 2030 agenda for sustainable development" (the "**UN Report**"):[35]

> Data collection and disaggregation that allow for comparison of population groups are central to a HRBA [human rights-based approach] to data and form part of States' human rights obligations.[36] Disaggregated data can inform on the extent of possible inequality and discrimination.

> We can only monitor progress if we have data that is disaggregated by sex, age, race, ethnicity, income, migration status, disability and other characteristics relating to the grounds of discrimination prohibited by human rights law. Only if we track progress for different population groups, in all countries, can we ensure that no one is indeed being left behind.'
>
> **Zeid Ra'ad Al Hussein,**
> **United Nations High Commissioner for Human Rights (2018)**

The UN Report notes that this was implicit in earlier treaties, but that "more recently adopted treaties make specific reference to the need for data collection and disaggregated statistics. See, for example, Article 31 of the Convention on the Rights of Persons with Disabilities."[37]

Many of the reports referred to above explicitly state that the GDPR should not be an obstacle for collecting this data. For example, in 2021 the EU High Level Group on Non-discrimination Equality and Diversity issued "Guidelines on improving the collection and use of equality data,"[38] which explicitly state:

> Sometimes data protection requirements are understood as prohibiting collection of personal data such as a person's ethnic origin, religion or sexual orientation. However, as the explanation below shows the European General Data Protection Regulation (GDPR), which is directly applicable in all EU Member States since May 2018, establishes conditions under which collection and processing of such data [are] allowed.

The UN Special Rapporteur on Extreme Poverty and Human Rights even opined that the European Commission should start an infringement procedure where a Member State continues to misinterpret data protection laws as not permitting data collection on the basis of racial and ethnic origin.[39]

---

[35] https://www.ohchr.org/sites/default/files/Documents/Issues/HRIndicators/GuidanceNoteonApproachtoData.pdf

[36] For instance, target 17.18 in the 2030 Agenda requests that Social Development Goals indicators are disaggregated by income, gender, age, race, ethnicity, migratory status, disability, geographic location, and other characteristics relevant in national contexts.

[37] See endnote n. 35, p. 15, footnote 27.

[38] EU High Level Group on Non-discrimination Equality and Diversity, "Guidelines on improving the collection and use of equality data," 2021, p.11, https://commission.europa.eu/system/files/2022-02/guidance_note_on_the_collection_and_use_of_equality_data_based_on_racial_or_ethnic_origin_final.pdf.

[39] United Nations, End-of-mission statement on Romania, Professor Philip Alston, United Nations Human Rights Council Special Rapporteur on Extreme Poverty and Human Rights, http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=16737&LangID=E#sthash.42v5AefT.dpuf.

In light of the above, employers referring to GDPR requirements to avoid collecting DEI data for monitoring purposes are starting to appear to be driven more by a wish to avoid workplace scrutiny than by genuine concerns for the privacy of their employees.[40] The employees whose privacy is at stake are exactly those who are potentially exposed to discrimination. At the risk of stating the obvious, invoking the GDPR as a prohibition on DEI data collection with the outcome that organizations avoid or are constrained from detecting discrimination of these groups, runs contrary to the GDPR's entire purpose. The GDPR is about preserving the privacy of the employees while protecting them against discrimination.

> The fifth myth is that GDPR precludes equality data. This is a dangerous myth, which is sometimes instrumentalised and used as an excuse. GDPR is actually a more sophisticated instrument than assumed and it is critical to consult with data protection authorities in crafting policies around data collection.
>
> **Michael O'Flaherty, Director of the Fundamental Rights Agency (FRA) (2021)**

Not surprisingly, the minority interest groups, who represent the groups whose privacy is actually at stake, actively advocate for such collection of data and monitoring.[41] If anything, their concerns as to collection of DEI data for DEI monitoring purposes is that these groups often do not feel represented in the **categorization** of the data collected.[42] If these are too generic or do not allow for splitting out of intersecting inequalities (like being female and from a minority), specific vulnerable groups may well fall outside the scope of DEI monitoring and therefore outside the scope of potential DEI policy measures. It is widely acknowledged that already the *setting of the categories* may represent bias, and the core principle of relevant human rights frameworks for collecting DEI data is to involve relevant minority stakeholders in a bottom-up process of indicator selection (the human rights principle of *participation*),[43] and further ensure data collection is based on the principle of *self-identification*, which

> "Without measuring and quantifying the extent of discrimination and inequalities in Europe, it becomes very difficult to tackle them effectively. Equality data can provide powerful tools against discrimination and exclusion, shedding light on the situation of groups that are at risk of discrimination. That's why we are calling for more data to measure discrimination and ensure equality in outcome."
>
> **European Network Against Racism, policy statement on website**

[40] Quote is from Michael O'Flaherty, Director of the Fundamental Rights Agency (FRA), Equality data round table report, 30 December 2021, https://commission.europa.eu/system/files/2021-12/roundtable-equality-data_post-event-report.pdf.

[41] See policy statement on the website of the European Network Against Racism (**ENAR**); as well as the statement dated 28 September 2022 issued by Equal@Work Partners calling on the EU to implement conducive legal frameworks that will bring operational and legal certainty to organizations willing to implement equality data collection measures on the grounds of race, ethnicity and other related categories., https://www.enar-eu.org/about/equality-data. See also https://www.enar-eu.org/equal-work-partners-call-on-the-eu-to-implement-proper-legal-frameworks-for/.

[42] For an excellent article on all issues related to ethnic categorization, see Bonnett, A., & Carrington, B. (2000), "Fitting into categories or falling between them? Rethinking ethnic classification," *British Journal of Sociology of Education*, 21(4), pp. 487–500.

[43] The Office of the United Nations High Commissioner for Human Rights (**OHCHR**), "Human Rights Indicators, A Guide to Measurement and Implementation," 2012, Chapter III sub. A (Ethical, statistical and human rights considerations in indicator selection), p. 46, https://www.ohchr.org/sites/default/files/Documents/Publications/Human_rights_indicators_en.pdf.

requires that surveys should always allow for free responses (including no responses) as well as indicating multiple identities (see section 5 on the human rights principle of self-identification).

> **Example –** Dutch organizations with more than 250 employees have the option to request DEI information from the Dutch Central Bureau of Statistics (**CBS**) about the cultural background of their workforce. The CBS, upon the request of the Dutch Ministry of Social Affairs and Employment, created the "Cultural Diversity Barometer." The Barometer allows employers to provide certain non-sensitive personal data to the CBS and, in turn, the CBS provides an anonymous statistical breakdown of the company's cultural diversity to the employers. This is split into three categories: employees with (i) a Dutch background, (ii) a western migration background, and (iii) a non-western migration background. Individuals are considered to have a migration background if at least one of their parents is born outside the Netherlands. A distinction is made between individuals born in a foreign country (first generation) and individuals who are born in the Netherlands (second generation). This terminology has been challenged as overly general.[44] The obvious issue here is that children of the second generation (i.e., the third generation) no longer qualify as having a migrant background, but may well belong to visible minorities and encounter discrimination in the workplace.[45] Another issue is that data are generally not available in a format that permits identification and analysis of multiple and intersecting disparities and discrimination. Individuals may experience discrimination and inequality along multiple axes (for example, gender and ethnic background). Analyzing data at the subgroup level allows for understanding of multiple and intersecting inequalities.[46] For example, research shows that lack of social networks and mentoring and sponsoring is a limiting factor for the promotion of women, but this is even stronger for cultural diversity, due to the lack of a "social bridging network," a network that allows for connections with other social groups.[47]

4. ESG reporting

[44] See Policy Brief 8 of the Netherlands Scientific Council for Government Policy "Abandon distinction western and non-western," as this distinction is not supported by science and is no longer informative, https://www.ser.nl/nl/thema/diversiteitinbedrijf/actueel/nieuws/CBS-westers-niet-westers and https://www.wrr.nl/publicaties/policy-briefs/2021/06/22/index

[45] The categorization has been reviewed and amended and will be implemented in 2023, see https://www.cbs.nl/nl-nl/longread/statistische-trends/2022/nieuwe-indeling-bevolking-naar-herkomst/4-de-nieuwe-indeling-naar-geboren-in-nederland-en-herkomstland. Migrant background is now split into four groups, with group two being the typical migration countries for the Netherlands, i.e., Turkey, Morocco, Surinam, Indonesia, and Dutch Caribbean. There is no category for third-generation migrants, so the flagged issue still applies.

[46] https://www.ohchr.org/sites/default/files/Documents/Issues/HRIndicators/GuidanceNoteonApproachtoData.pdf, p. 14.

[47] Putnam, R.D. (2007) "E Pluribus Unum: Diversity and Community in the Twenty-first Century," Scandinavian Political Studies, 30 (2), pp. 137–174.

Under the upcoming CSRD,[48] large companies[49] will be subject to mandatory disclosure requirements on ESG matters from 2024 onwards (i.e., in their annual reports published in 2025).[50] The European Commission is tasked with setting the reporting standards and has asked the European Financial Reporting Advisory Group (**EFRAG**) to provide recommendations for these standards. In November 2022, EFRAG published the first draft standards. The European Commission is now consulting relevant EU bodies and Member States, before adopting the standards as delegated acts in June 2023.

One of the draft reporting standards provides for a standard on reporting on a company's own workforce (European Sustainability Reporting Standard S1 (**ESRS S1)**).[51] This standard requires a general explanation of the company's approach identifying and managing any material, actual, and potential impacts on its own workforce in relation to *equal treatment and opportunities for all*, including "gender equality and equal pay for work of equal value" and "diversity." From the definitions in ESRS S1, it is clear that "equal treatment" requires that there shall be "no direct or indirect discrimination based on criteria such as gender and racial or ethnic origin; "equal opportunities" refers to equal and nondiscriminatory access to opportunities for education, training, employment, career development and the exercise of power without any individuals being disadvantaged on the basis of criteria such as gender and racial or ethnic origin.

ESRS S1 provides a specific chapter on metrics and targets, which requires mandatory **public** reporting metrics on a set of specific characteristics of a company's workforce, which does include gender, but not racial or ethnic origin.[52] Reading all standards, however, it is difficult to imagine how companies could report on the standards without collecting and monitoring DEI data **internally**.

---

[48] See Corporate Sustainability Reporting Directive (Nov. 10, 2022), at point (4) of Article 1, available at https://www.europarl.europa.eu/doceo/document/TA-9-2022-0380_EN.pdf.

[49] The new EU sustainability reporting requirements will apply to all large companies that fulfill two of the following three criteria: more than 250 employees, €40 million net revenue, and more than €20 million on the balance sheet), whether listed or not. Lighter reporting standards will apply to small and medium enterprises listed on public markets.

[50] See Article 1 (Amendments to Directive 2013/34/EU) sub. (8), which introduces new Chapter 6a Sustainability Reporting Standards, pursuant to which the European Commission will adopt a delegated act, specifying the information that undertakings are to disclose about social and human factors, which include equal treatment and opportunity for all, including diversity provisions.

[51] See European Financial Reporting Advisory Group, Draft European Sustainability Reporting Standard S1 Own Workforce, Nov. 2022, https://efrag.org/Assets/Download?assetUrl=%2Fsites%2Fwebpublishing%2FSiteAssets%2F13%2520Draft%2520ESRS%2520S1%2520Own%2520workforce%2520November%25202022.pdf&AspxAutoDetectCookieSupport=1

[52] The initial working draft of ESRS S1 published by EFRAG for public consultation did include a public reporting requirement also of the total number of 'employees belonging to vulnerable groups, where relevant and legally permissible to report' (see disclosure requirement 11), Download (efrag.org). This requirement was deleted from the draft standards presented by EFRAG to the European Commission. The European Network Against Racism has written an open letter to the European Commission, urging the Commission to again include public reporting on a breakdown of a company's workforce based on racial and ethnic background: 'We underline the importance of being able to measure at all levels of the company. This is because it is not uncommon in sectors that individuals who are part of racialised communities are overrepresented in the lower rungs of an organisation, and completely absent at the higher rungs.'

For example, the general disclosure requirements of ESRS S1 require the company to disclose all of its policies relating to equal treatment and opportunity,[53] including:

a) Whether it has specific policies aimed at the elimination of discrimination, including harassment, and promoting equal opportunities and other ways to advance diversity and inclusion;
b) Whether the following grounds for discrimination and diversity are specifically covered in the policy: racial and ethnic origin, color, sex, sexual orientation, gender identity, disability, age, religion, political opinion, national extraction or social origin, and any other forms of discrimination covered by EU regulation and national law;
c) Whether the undertaking has specific policy commitments related to inclusion and/or affirmative action for people from groups at particular risk of vulnerability in its own workforce and, if so, what these commitments are; and
d) Whether and how these policies are implemented through specific procedures to ensure discrimination is prevented, mitigated, and acted upon once detected, as well as to advance diversity and inclusion in general.

It is difficult to see how companies can comply with reporting the information in clause (d) which requires reporting **how** the policies are implemented **to ensure discrimination is prevented, mitigated, and acted upon once detected**, without collecting DEI data.

ESRS S1 further requires an explanation of how the company's dependencies on its own workforce can create material risks or opportunities for the undertaking. It provides the following: "For example, on the matter of equal opportunities, discrimination in hiring and promotion against women can reduce the undertaking's access to qualified labour and harm its reputation." The example relates to gender, but would obviously be equally valid for discrimination based on racial or ethnic origin.

ESRS S1 further clarifies how disclosures under S1 relate to disclosures under ESRS S2, which includes disclosures where potential impacts on a company's own workforce have an impact on the company's strategy and business model(s). See:

> **Appendix B.1** to S1 Application Requirements for ESRS 2 related disclosures, which includes
>
> > "**Diversity**. Representation of women and/or ethnic groups or minorities in own workforce. Age distribution in own workforce. Percentage of persons with disabilities within the own workforce."
>
> **Appendix B.3**: Application Requirements for ESRS S1–4 "Taking action on material impacts on own workforce, and approaches to mitigating material risks and pursuing material opportunities related to own workforce, and effectiveness of those actions," which includes:
>
> > "**Diversity**. Training on diversity and inclusion (including ethnicity considerations), targeted recruitment of underrepresented groups".

[53] See S1-1 – Policies related to own workforce.

> **Appendix B.4**: Application Requirements for ESRS S1–5 "Targets related to managing material negative impacts, advancing positive impacts, and managing material risks and opportunities," which includes:
>
> > "**Diversity**. Increasing the % of underrepresented groups in own workforce and top management."

Based on the reporting requirements above, collecting and monitoring of DEI data will be required for mandatory disclosures, which also provides for a legal basis under the GDPR for collecting such data, provided the other provisions of GDPR are complied with as well as broader human rights principles. Before setting out the GDPR requirements, a brief summary is provided of the broader human rights principles that apply to data collection of DEI data for monitoring purposes.

5. Human rights principles

The three main human rights principles in relation to data collection processes are self-identification, participation, and data protection.[54] The principle of self-identification requires that people should have the option of self-identifying when confronted with a question seeking sensitive personal information related to them. As early as 1990, the Committee on the Elimination of Racial Discrimination held that identification as a member of a particular ethnic group "shall, if no justification exists to the contrary, be based upon self-identification by the individual concerned."[55] A personal sense of identity and belonging cannot in principle be restricted or undermined by a government-imposed identity and should not be assigned through imputation or proxy. This entails that all questions on personal identity, whether in surveys or administrative data, should allow for free responses (including no response) as well as multiple identities.[56] Also, owing to the sensitive nature of survey questions on population characteristics, special care is required by data collectors to demonstrate to respondents that appropriate data protection and disclosure control measures are in place.[57]

6. EU data protection law requirements

Collecting racial or ethnic data for monitoring is rightfully described in literature as "a problematic necessity, a process that itself needs constant monitoring."[58] The collection and use of racial and ethnic data to combat discrimination is not an "innocent" practice.[59] Even if performed on an

---

[54] The Office of the United Nations High Commissioner for Human Rights (**OHCHR**), Human Rights Indicators, A Guide to Measurement and Implementation, 2012, p. 46, https://www.ohchr.org/sites/default/files/Documents/Publications/Human_rights_indicators_en.pdf.

[55] General Recommendation 8, Membership of racial or ethnic groups based on self-identification, 1990, https://www.legal-tools.org/doc/2503f1/pdf/.

[56] https://www.ohchr.org/sites/default/files/Documents/Issues/HRIndicators/GuidanceNoteonApproachtoData.pdf, pp. 12–13. See also The EU High Level Group on Non-discrimination Equality and Diversity, "Guidelines on improving the collection and use of equality data," 2021, p.11, https://commission.europa.eu/system/files/2022-02/guidance_note_on_the_collection_and_use_of_equality_data_based_on_racial_or_ethnic_origin_final.pdf.

[57] OHCHR Guide, p. 48.

[58] Bonnett and Carrington 2000, p. 488.

[59] The Dutch Young Academy, Antidiscrimination data collection in academia: and exploration of survey methodology practices outside of the Netherlands, https://www.dejongeakademie.nl/en/publications/2300840.aspx?t=Antidiscrimination-data-practices-worldwide-and-views-of-students-and-staff-of-colour.

anonymized or aggregated basis, it can contribute to exclusion and discrimination. An example is when politicians argue, based on statistics, that there are "too many" people of a certain category in a country.[60]

Collection and processing of racial and ethnic data is not illegal in the EU. In general, no Member State imposes an absolute prohibition on collecting this data.[61] There is also no general requirement under the Racial Equality Directive to collect, analyze, and use equality data. Obligations to collect racial or ethnic data also do not generally seem to be codified in law in the Member States, with notable exceptions in Finland, Ireland and (pre-Brexit) the UK.[62]

In the absence of specific prohibitions and specific requirements in EU and Member State law, processing of racial and ethnic data is governed by the GDPR, which provides a special regime for processing "special categories of data" such as data revealing racial or ethnic origin.[63]/[64]

Article 9 of the GDPR prohibits the processing of special categories of data, with notable exceptions. The prohibition does not apply (insofar as relevant here)[65] when:

---

[60] See older examples in Bonnett and Carrington 2000.

[61] European Commission, Analysis and comparative review of equality data collection practices in the European Union Data collection in the field of ethnicity, p. 14, https://commission.europa.eu/system/files/2021-09/data_collection_in_the_field_of_ethnicity.pdf. Even in France, often seen as a case of absolute prohibition, ethnic data collection is possible under certain exceptions. The same applies to Italy. Italian Workers' Statute (Italian Law No. 300/1970), Article 8, expressly forbids employers from collecting and using ethnic data to decide whether to hire a candidate and to decide any other aspect of the employment relationship already in place (like promotions). Collecting such data for monitoring workplace discrimination and equal opportunity falls outside the prohibition (provided it is ensured such data cannot be used for other purposes).

[62] Three notable exceptions, Finland, Ireland and the UK (before leaving the EU), place a duty of equality data collection on public bodies as part of their equality planning, see https://ec.europa.eu/info/sites/default/files/data_collection_in_the_field_of_ethnicity.pdf, p. 16.

[63] Data revealing racial or ethnic origin qualifies as a "special category" of personal data under Article 9 of the GDPR. Data on nationality or place of birth of a person or their parents do not qualify as special categories of data and can as a rule be collected without consent of the surveyed respondent. However, if they are used to predict ethnic or racial origin, they become subject to the regime of Article 9 GDPR for processing special categories of data.

[64] There is no debate that the summary of requirements here is a correct reflection of the requirements of the GDPR. A similar summary of relevant provisions of the EU High Level Group on Non-discrimination, Equality, and Diversity can be found in its 2021 guidelines, p. 12, https://ec.europa.eu/info/sites/default/files/en-guidelines-improving-collection-and-use-of-equality-data.pdf and further in its 2021 Guidance Note on the collection and use of equality data based on racial or ethnic origin, p. 30, https://commission.europa.eu/system/files/2022-02/guidance_note_on_the_collection_and_use_of_equality_data_based_on_racial_or_ethnic_origin_final.pdf. See further the guidelines issued by the Dutch Social Economic Council in Dec. 2021, "Meten is Weten, zicht op effecten van diversiteits- en inclusiebeleid," Charter Document, pp. 7– 10, Dec. 2021; and an earlier report by PWC on assignment of the Dutch government, "Onderzoek Vrijwllige vastlegging van culturele diversiteit," https://www.rijksoverheid.nl/documenten/publicaties/2017/12/22/onderzoek-vrijwillige-vastlegging-van-culturele-diversiteit.

[65] Note that Article 9(2)(b) of the GDPR provides a condition for collecting racial and ethnic data where it "*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 … in so far as it is authorised by Union or Member State law….*" There is currently no Union or Member State law that provides for an employer obligation to collect racial or ethnic data for monitoring purposes. However, EU legislators considered this to be a valid exception for Member States to implement in their national laws. Art. 88 of the GDPR states that Member States may, by law or collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms of employees with respect to the processing of

- The individual has given **explicit consent** to the processing of personal data for one or more specified purposes, except where EU or Member State law provides that the prohibition may not be lifted by the individual (Article 9(2) sub. (a) GDPR).

- The processing is necessary for reasons of **substantial public interest** on the basis of EU or Member State law (Article 9(2) sub. (g) GDPR).

- The processing is necessary for **statistical purposes** in accordance with Article 89(1) GDPR based on EU or Member State law (Article 9(2) sub. (j) GDPR).

For the conditions to apply, provisions must be made in EU or Member State law which permit processing where necessary for substantial public interest or statistical purposes. In practice, most Member States have **not** used their discretionary power under the GDPR to provide a specific legal basis in their national law for processing racial or ethnic data for these purposes.[66] Member States have, however, also **not** used the possibility under GDPR to provide in their national law that the prohibition under Article 9 may **not** be lifted by consent. This leaves explicit consent as a valid, but also the only practically viable, option to collect DEI data for monitoring purposes.[67] This is in line with human rights principles, provided reporting is based on self-identification.

Once the CDRD has been implemented in the national laws of the Member States, collecting DEI data will be required for mandatory ESG disclosures, which will be permitted under Article 9(2) sub. (g) GDPR (reason of substantial public interest). Where organizations collect this data the human rights principles set out above should be observed, in particular that reporting should be based on self-identification. In practice, the legal basis of substantial public interest, will therefore very much mirror the legal basis of explicit consent and the safeguards and mitigating measures set out below will equally apply.

6.1. Explicit consent

employees' personal data in the employment context. In particular, these rules may be provided for the purposes of, *inter alia*, equality and diversity in the workplace.

[66] A notable exception is the UK, which, during its time in the EU, legislated that the collection of racial and ethnic data would meet the requirements of *the substantial public interest* condition for purposes of both "Equality of opportunity or treatment" and "Racial and ethnic diversity at senior levels" and further provided criteria for processing ethnic data for *statistical purposes*, see Schedule 1 to the UK Data Protection Act 2018, and the Information Commissioner's Office, Guidance on special category data, 2018. Schedule 1 also provides specific criteria for meeting the requirements of the statistical purposes condition, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/. Another exception is the Netherlands, which allows for a limited processing of racial and ethnic data (limited to country of birth and parents' or grandparents' countries of birth) for reasons of *substantial public interest.*

[67] For example, in the Netherlands, it is generally accepted that collecting DEI data can take place on a voluntary basis, see Dutch Social Economic Council, Dec. 2021, "Meten is Weten, zicht op effecten van diversiteits- en inclusiebeleid," Charter Document, pp. 7–10, Dec. 2021. See also the report titled "Het moet wel werken," p. 30, https://goldschmeding.foundation/wp-content/uploads/Rapport-Het-Moet-Wel-Werken-Vergelijkende-analyse-juli-2021.pdf.

The requirements for valid consent are strict, especially in the workplace.[68] For instance, consent must be 'freely given', which is considered problematic in view of the imbalance of power between the employer and the individual.[69] The term 'explicit' refers to the way consent is expressed by the individual. It means that the data subject must give an express statement of consent. An obvious way to make sure consent is explicit would be to expressly confirm consent in a written statement, an electronic form or in an email.[70]

For employee consent to be valid, employees need to have genuine free choice as whether to provide the information or not without any detrimental effects. This includes no downside whatsoever to an employee refusing to provide consent, which would be the case if refusal of consent would, for example, exclude the employee from any positive action initiatives.[71] To ensure that consent is indeed freely given, the voluntary nature of the reporting for employees should be twofold: (1) the act of completing a survey or questionnaire related to one's racial or ethnic background should be voluntary and (2) the survey or questionnaire should include options for the employee to respond with (an equivalent of) "I choose not to say." The individual status of a survey or questionnaire (i.e., completed or not completed), as well as the provided answers, should not be visible to the employer on an individual basis. This is in practice realized by *privacy-by-design* measures (see further below).

Note that for consent to be valid, it needs to be accompanied with clear information as to why it is being collected and how it will be used (consent needs to be "*specific and informed*").[72] In addition, employees should be informed that consent can be withdrawn at any time and that any withdrawal of consent will not affect the lawfulness of processing prior to the withdrawal.[73]

When consent is withdrawn, any processing of personal data (to the extent it is identifiable) will need to stop from the moment that the consent is withdrawn. However, where data are collected and processed in the aggregate (see section 6.2 below on privacy-by-design requirements), employees will no longer be identifiable or traceable, and, therefore, any withdrawal of consent will not be effective in relation to data already collected and included in such reports.

6.2. General data protection principles

Obtaining consent does not negate or in any way diminish the data controller's obligations to observe the principles of processing enshrined in the GDPR, especially Article 5 of the GDPR with regard to fairness, necessity, and proportionality, as well as data quality.[74] Employers will

[68] Article 4(11) of the GDPR defines consent as "any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."
[69] Guidance of the European Data Protection Board has made it explicit in a series of guidance documents that, for the majority of data processing at work, consent is not a suitable legal basis due to the nature of the relationship between employer and employee. See also Opinion 2/2017 on data processing at work (**WP249**), paragraph 3.3.1.6.2, at https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf.
[70] EDPB Guidelines 05/2020 on consent under Regulation 2016/679, adopted on May 4, 2020, p. 21, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf.
[71] See WP249, paragraph 6.2.
[72] EDPB Guidelines 05/2020 on consent under Regulation 2016/679, adopted on May 4, 2020, pp. 13–15.
[73] Article 7(3) GDPR.
[74] EDPB Guidelines 05/2020 on consent under Regulation 2016/679, adopted on May 4, 2020, p. 5.

further have to comply with principles of privacy-by-design.[75] In practice, this means that employers should only process the personal data that they strictly need for their pursued purposes and in the most privacy-friendly manner. For example, employers can collect DEI data without reference to individual employees (i.e., without employees providing their name, or other unique identifier, such as a personnel number or email address). In this manner, employers will comply with data minimization and privacy-by-design requirements, limiting any impact on the privacy of their employees. In practice we see also that employers involve a third-party service provider, and request employees to send the information directly to the third-party provider. The third-party service provider subsequently only shares aggregate information with the employer.

From a technical perspective, it is possible to achieve a similar segregation of duties within the company's internal HR system (like Workday or SuccessFactors), whereby data are collected on a de-identified basis and only one or two employees within the diversity function have access to de-identified DEI data for statistical analysis and subsequently report to management on an aggregate basis only (ensuring individual employees cannot be singled out or re-identified).[76] This requires customization of HR systems, which is currently underway. Where employers have a works council, the works council will need to provide its prior approval for any company policy related to the processing of employee data. As part of the works council approval process, the privacy-by-design measures can be verified.

For the sake of completeness, note that where data collection and processing are on a truly anonymous basis, the provisions of the GDPR would not apply.[77] The threshold under the GDPR for data to be truly anonymous is, however, very high and is unlikely to be met where employers collect such data from their employees. Any application of anonymization techniques, such as pseudonymization (e.g., removal or replacement of unique identifiers and names) therefore do not take the data processing outside the scope of the GDPR, but are rather necessary measures to meet data minimization and privacy-by-design requirements.

7. The way forward

It is no longer possible to hide behind the GDPR to avoid collecting DEI data for monitoring purposes. The direction of travel is towards meaningful DEI policies, monitoring, and reporting (such as under CSRD). Collecting data relating to racial and ethnic origin has been labeled "a problematic necessity, a process that itself needs constant monitoring." This is the negative way of qualifying DEI data collection and monitoring. A positive human rights-based approach is that data-collection processes should be based on *self-identification*, *participation*, and *data protection*. Where all three principles are safeguarded, the process will be controlled and can be trusted without being inherently problematic or in need of constant monitoring. The path forward revolves around building trust with the workforce (and their works councils and trade unions). If trust is not

[75] Article 25 GDPR.
[76] See Article 29 Working Party Opinion 05/2014 on Anonymization Techniques, adopted on 10 April 2014.
[77] Recital 26 of the GDPR states the principles of data protection should not apply to anonymous information which does not relate to an identified or identifiable natural person, or which relates to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. Recital 26 further states that the GDPR does not concern the processing of such anonymous information, including for statistical or research purposes.

already a given, the recommendation is to start small (in less sensitive jurisdictions), engage with works councils or the workforce at large, and in light of the upcoming CRSD, start now.[78]

Self-identification: A company requires the full trust of its employees to be able to collect representative DEI data from them based on self-identification. If introduction of DEI data collection is perceived by employees as abrupt and countercultural, or a box-ticking exercise unlikely to result in meaningful change, surveys will not be successful. For employees to fill out surveys disclosing sensitive data, trust is required that their employer is serious about its DEI efforts and that data collection and monitoring **complements** these efforts based on the aphorism "We measure what we treasure." Practice shows that when a certain tipping point is reached, employees are proud to self-identify and contribute to the DEI statistics of their company.

Trust will be undermined if employees do not recognize themselves in any pre-defined categories. Proper self-identification entails that any pre-defined categories are relevant to a country's workforce, allow for free responses (including no response) as well as allow for identifying with multiple identities. Other protections and features involved in surveys to make them both more effective in representing diversity, and more acceptable to employees are:[79]

- Offering the possibility to update the information they have provided.
- Offering the possibility to elaborate on answers given.
- Acknowledging that there are far more possible identifications than realistically could be accounted for in the surveys.
- Giving the broader objective of the survey, including on the envisaged reporting metrics (see further below) as well as information how the company will report on effectiveness of any follow-up actions, including any lessons learned.
- Clarity on data use and management: binding statements on access and purpose limitation, (specifying the ways in which information will (and will not) be used (see further below on data protection).

Trust of employees will be enhanced, if the company has put careful thought into the reporting metrics, ensuring that reporting can actually inform where the company can focus interventions to bring about meaningful change. For example, is important to ensure reporting metrics are not just *outcome-based* (tracking demographics, without knowing where a problem exists), but are also *process-based.* Process-based metrics can pinpoint problems in employee-management processes such as hiring, evaluation, promotion, and executive sponsorship. If *outcome* metrics inform a company that it has limited percentages of specific minorities, *process* metrics may show in which part of its processes (or part of a process, e.g., which part of the hiring process) a company needs to focus to bring about meaningful change. Examples of these metrics include the speed at which

[78] For an informative article on the practicalities of implementing data-driven diversity proposals, see Data-Driven Diversity (hbr.org). The distinction between outcome-based and process-based metrics is based on this article.
[79] The Dutch Young Academy, Antidiscrimination data collection in academia: and exploration of survey methodology practices outside of the Netherlands, p. 4- 5, https://www.dejongeakademie.nl/en/publications/2300840.aspx?t=Antidiscrimination-data-practices-worldwide-and-views-of-students-and-staff-of-colour

minorities move up the corporate ladder and salary differentials between different categories in comparable jobs.

Participation: Trust requires an inclusive bottom-up process whereby employees (and their works councils) have a say in the data collection and monitoring procedure. For example, in setting the categories in a survey to ensure minority employees can 'recognize' themselves in those categories, in setting the reporting metrics to ensure these may bring about meaningful change as well as in setting the data protection safeguards (see below).

Data protection: To gain employees' trust, data protection principles, such as data security, data minimization and privacy-by-design, must be fully implemented. A company will need to submit a data collection and processing protocol to its works council and receive its approval, specifying all organizational, contractual and technical measures ensuring that data are collected on a de-identified basis, and access controls are in place to ensure access to the data is limited to one or two employees of the diversity team in order to generate statistics only.

Country reports

Below we provide a summary of the legal basis available under the laws of France, Germany, Italy, Spain and The Netherlands, and available to collect racial and ethnic background data of their employees for purposes of monitoring their DEI policies (**DEI Monitoring Purposes**). Note that in all cases also the general data processing principles apply (such as privacy-by-design requirements) as set out in section 6.2, but are not repeated here.

France

Héléna Delabarre & Sylvain Naillat, ***Nomos, Société D'Avocats***

Summary requirements for processing racial and ethnic background data

Under French law, the processing of race and ethnicity data is prohibited *in principle* under (i) a general provision of the French Constitution, and (ii) some specific provisions of French data protection laws, which is also the public position of the French Data Protection Authority's (**CNIL**). French law does not recognize any categorization of people based on their (alleged) races or ethnicity and the prohibition of processing race and ethnicity data has been reaffirmed by the French Constitutional Court in a decision related to public studies whose purpose was to measure diversity/minority groups. However, while race and ethnicity data may not be collected or processed, objective criteria relating to geographical and/or cultural **origins**, such as name, nationality, birthplace, mother tongue, etc., can be considered by employers in order to measure diversity and to fight against discrimination. In a public paper from 2012[80] (that has not been contradicted since) the CNIL confirmed that employers may collect and process data about objective criteria relating to "**origin**," such as the birthplace of the respondent and his/her parents, his/her mother tongue, his/her

[80] https://www.cnil.fr/sites/default/files/atoms/files/ddd_gui_20120501_egalite_chances_0.pdf.

nationality and that of his/her parents, etc., if such processing is necessary for the purpose of conducting statistical studies aiming at measuring and fighting discrimination. The CNIL also considers that questions about self-identification and how the respondent feels perceived by others can be asked if necessary, in view of the purpose of the data collection and any other questions asked. See the CNIL's paper:

> *In accordance with the decision of the Constitutional Court of 15 November 2007 and the insights of the Cahiers du Conseil, studies on the measurement of diversity cannot, without violating Article 1 of the Constitution, be based on the ethnic or racial origins of the persons. Any nomenclature that could be interpreted as ethno-racial reference must therefore be avoided.* ***It is nevertheless possible to approach the criterion of "origin" on the basis of objective data such as the place of birth and the nationality at birth of the respondent and his or her parents, but also, if necessary, on the basis of subjective data relating to how the respondent self-identifies or how the person feels perceived by others***.[81]

Based on the guidance from the CNIL, several public studies have been conducted relying on the collection of information considered permissible by the CNIL, i.e., (i) whether or not respondents *felt discriminated against* based on their origins or skin colour; (ii) how the respondent self-identifies; and (iii) statistics about the *geographical and/or cultural origins* of the respondents.[82] The provision of any information should be entirely voluntary and the rules regarding explicit consent in section 6.1 above apply in the same manner to France. Any questions relating to the collection of data regarding geographical and/or cultural origins should be objective, and in the absence of the need to identify (directly or indirectly) the individuals, then the collection process should be entirely anonymous.

Germany

Hanno Timner, ***Morrison & Foerster***

Legal basis for processing racial and ethnic background data

Under German law, there is neither a specific legal requirement for employers to collect racial and ethnic background data of their employees, nor is there a general prohibition for employers to collect such data.

Employers in Germany can lawfully process racial and ethnic background data for DEI Monitoring Purposes on the basis of (i) necessity to exercise their labour law rights and obligations or (ii) based on explicit consent of their employees. If the employer has a works council, the works council has a co-determination right for the implementation of diversity surveys and questionnaires in accordance with Section 94 of the Works Council Act (*Betriebsverfassungsgesetz* – "**BetrVG**") if the information is not collected anonymously and on a voluntary basis. If the information is collected electronically, the works council may have a co-determination right in accordance with Section 87(1), no. 6 BetrVG.

---

[81] https://www.cnil.fr/sites/default/files/atoms/files/ddd_gui_20120501_egalite_chances_0.pdf (page 70).

[82] This article from the workers union "CGT," refers to a study conducted by the "Défenseur des droits" (a public body) who notably co-signed the CNIL's 2012 paper referred to in footnotes 80 and 81 above. https://www.cgt.fr/actualites/france/interprofessionnel/discriminations/le-defenseur-des-droits-denonce-un-racisme. *See also* recent studies conducted by the public institutions INED and INSEE: https://teo.site.ined.fr/fichier/s_rubrique/29262/teo2_questionnaire.fr.pdf

Necessity to exercise labour law rights or obligations. According to Section 26(3) of the German Federal Data Protection Act (*Bundesdatenschutzgesetz* – "**BDSG**"), the processing of racial and ethnic background data in the employment context is only permitted if the processing is necessary for the employer to exercise rights or comply with legal obligations derived from labour law, social security, and social protection law, and there is no reason to believe that the data subject has an overriding legitimate interest in not processing the data. One of the rights of the employer derives from Section 5 of the German General Equal Treatment Act (*Allgemeines Gleichbehandlungsgesetz* – "**AGG**"), according to which employers have the right to adopt positive measures to prevent and stop discrimination on the grounds of race or ethnicity. As a precondition to the adoption of such measures, employers may collect data to identify their DEI needs.

Explicit consent. For all other purposes of processing racial and ethnic background data, employers will have to rely on explicit consent and voluntary reporting by employees. We refer to the conditions for explicit consent set out above in section 6.1, as they apply in the same manner to Germany. Further, Section 26(2) BDSG specifies that the employee's level of dependence in the employment relationship and the circumstances under which consent was given have to be taken into account when assessing whether an employee's consent was freely given. According to Section 26(2) BDSG, consent may be freely given, in particular, if it is associated with a legal or economic advantage for the employee, or if the employer and the employee are pursuing the same interests. This can be the case if the collection of data also benefits employees, e.g., if it leads to the establishment of comprehensive DEI management within the employer's company.

Italy

Marco Tesoro, ***Tesoro and Partners***

Summary requirements for processing racial and ethnic background data

The Italian Data Protection Code (**IDPC**) regulates the processing of personal data under Article 9 of the GDPR, stating that the legal basis for the processing of such data must be to comply with a law or regulation (art. 2-*ter*(1), IDPC), or for reasons of relevant public interest. Under Italian law, no specific legal basis has been implemented to process racial or ethnic data for reasons of public interest.

Explicit consent. We refer to the conditions for explicit consent set out above in section 6.1, as they apply in the same manner to Italy. The IDPC does not expressly exclude the possibility of processing racial and ethnicity data based on employees' consent. Employers wanting to collect and process racial and ethnicity data on the basis of employees' consent under Art. 9 of the GDPR, however, should ensure that the consent is granted on a free basis and, where possible, involve the trade unions they are associated with (as well as their Works Council, where relevant). The trade unions should be able to i) ascertain and certify that the employees' consent has been freely given; and ii) ensure that employees are fully aware of their rights and of the consequences of providing such data. In the absence of associated trade unions, employers may inform the local representative of the union associations who signed the collective bargaining agreement (**CBA**) that applies (if any). Furthermore, employers should ensure that employees are given the option to "*prefer not to say*."

Statute of Workers. It is also worth noting that under Italian law, there is a general prohibition on the collection of information not strictly related or needed to assess the

employee's professional capability. Per Article 8, Law 23 May 1970, no. 300 "**Statute of Workers**," race and ethnicity data should not be collected or used by employers to impact in any way the decision to hire a candidate or to manage any of the terms of the employment relationship.

Spain

Laura Castillo, ***Gómez-Acebo & Pombo***

Summary requirements for processing racial and ethnic background data

Under the Organic Law 3/2018 of 5th December on the Protection of Personal Data and Guarantee of Digital Rights (**SDPL**), there is a general prohibition on collecting racial and ethnic background information unless: (i) there is a legal requirement to do so (per Article 9 of the SDPL); or (ii) the employees have provided their explicit consent (although the latter is not without risk).

Fulfilment of a legal requirement. The Comprehensive Law 15/2022 of 12th July, for Equal Treatment and Non-Discrimination (the "**Equal Treatment Law**") guarantees and promotes the right to equal treatment and non-discrimination. This Law expressly states that no limitations, segregations, or exclusions may be made based on ethnicity or racial backgrounds, i.e., nobody can be discriminated against on grounds of race or ethnicity. In this context, any positive discrimination measures that have been implemented as a result of the Equal Treatment Law have been included in collective bargaining agreements (**CBA**) or collective agreements as agreed with the unions or the relevant employee representatives. Where there is a requirement in the CBA to collect race and ethnicity data from employees, employers can do so, as this would constitute a legal requirement. In circumstances where the CBA does not specifically require the collection of this type of information, employers can either seek to include such a provision in the terms of the CBA or a collective agreement and work with the unions or legal representatives to do so, or take an alternative approach and rely on explicit consent, as set out immediately below.

Explicit consent. In principle, an employee's consent on its own is not sufficient to lift the general prohibition on the processing of sensitive data under the SDPL. However, one of the main aims of the prohibition pursuant to the SDPL is to avoid discrimination. Therefore, if the purpose of collection is to promote diversity, it is arguable (although this has not yet been tested in Spain) that employers can rely on explicit consent, and we refer to the conditions for explicit consent set out above in section 6.1, as they apply in the same manner to Spain. In addition to the conditions in section 6.1, Spanish case law has determined that the employee's level of dependence within the employment relationship and the circumstances under which consent is given should be considered when assessing whether an employee's consent is freely given. It is therefore not recommended that employers obtain or process race and ethnicity data of its employees during the recruitment or hiring process, or before the end of the probationary period, unless a CBA regulates this issue in a different manner. Employers should also ensure that employees are given the option to "prefer not to say" and ensure that they are able to prove that consent is genuinely voluntary, as explained in section 6.1 above.

The Netherlands

Marta Hovanesian, ***Morrison & Foerster***

Summary requirements for processing racial and ethnic background data

Under Dutch law, there is neither a specific legal requirement for employers to collect racial and ethnic background data of their employees, nor is there a general prohibition for employers to collect such data.

Employers in the Netherlands can lawfully process racial and ethnic background data of their employees for DEI Monitoring Purposes on the basis of (i) the substantial public interest on the basis of Dutch law or (ii) the explicit consent of the employees. Employers with a works council need to ensure their works council approves any policy related to processing Equality Data.

Substantial public interest. The Netherlands has implemented the conditions of Article 9(2) GDPR for the processing of racial and ethnic background data in the Dutch GDPR Implementation Act (the "**Dutch Implementation Act**"). More specifically, Article 25 of the Dutch Implementation Act provides that racial and ethnicity background data (limited to country of birth and parents' or grandparents' countries of birth) may be processed (on the basis of substantial public interest) if processing is necessary for the purpose of restoring a disadvantaged position of a minority group, and only if the individual has not objected to the processing. Reliance on this condition requires the employer to, among other things, (i) demonstrate that certain groups of people have a disadvantaged position; (ii) implement a wider company policy aimed at restoring this disadvantage; and (iii) demonstrate that the processing of race and ethnicity data is necessary for the implementation and execution of said policy.

Explicit consent. Employers can collect racial and ethnicity background data of their employees for DEI Monitoring Purposes based on explicit consent and voluntary reporting by employees. The conditions for consent set out above in section 6.1 apply in the same manner to the Netherlands.

Cultural Diversity Barometer. Note that Dutch employers with more than 250 employees have the option to request DEI information from Statistics Netherlands about their own company. Statistics Netherlands, upon the Ministry of Social Affairs and Employment's request, created the "Cultural Diversity Barometer". The Barometer allows employers to disclose certain non-sensitive personal data to Statistics Netherlands, which, in turn, will report back to the relevant employers with a statistical and anonymous overview of the company's cultural diversity (e.g., percentage of employees with a (i) Dutch background, (ii) western migration background, and (iii) non-western migration background). Statistics Netherlands can either provide information about the cultural diversity within the entire organization or within specific departments of the organization (provided that the individual departments have more than 250 employees).

***