BrightTALK Original

Privacy Insight Series:

HR Privacy – Protecting Privacy in Global Diversity and Inclusion Initiatives

Hosts

Bret Cohen
Partner
Hogan Lovells US LLP

Jackie Wilkosz
Manager
Aleada Consulting

Agenda

Part I:

- US and EU legal landscape
- Common legal challenges
- Best practices—legal compliance strategy

Part II:

- Developing and implementing a D&I Program
- HR Data Analytics
- Best practices—implementation strategy

Privacy and Diversity Initiatives

- Privacy laws restrict the processing of sensitive categories of data, including race, ethnicity, and sexual orientation
- At the same time, sensitive categories of data are a critical component of diversity initiatives, and to further policies against non-discrimination
- Some countries maintain specific quotas regarding workforce composition, requiring employers to collect certain information to prove compliance

How do we reconcile?

What Data is Diversity-Related?

Diversity Program Examples

- The Rooney Rule requires every National Football League team to interview at least one minority candidate for head coach vacancies
- The Mansfield Rule measures whether law firms have considered women, LGBTQ+, and minority lawyers in their promotions decisions

Diversity Data Examples

- Age
- Gender
- Physical challenges or disabilities
- Racial or ethnic origin
- Sexual orientation

United States

- U.S. federal regulations require companies with 100 or more workers (subject to Title VII of the Civil Rights Act of 1964) to file certain demographic information
- EEOC recommends anonymous self-reporting and recommends:
  - Employers should resurvey employees periodically or request employees update their information on an intranet page to ensure its information is accurate and up-to-date
  - Employers should allow employees to self-identify, and not question the self-identification even if they believe the employee to be of a different race or ethnicity
  - If an employee refuses to self-identify, the employer should use existing employment records or visual observation to make an educated determination

European Union: Non-Sensitive Data

- Art. 6 – Lawfulness of Processing
  - Processing shall be lawful only if and to the extent that at least one of the following applies:
    - the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
    - processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
    - processing is necessary for compliance with a legal obligation to which the controller is subject;
    - processing is necessary in order to protect the vital interests of the data subject or of another natural person;
    - processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
    - processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

European Union: Sensitive Data

- Art. 9 – Processing of Special Categories of Personal Data
  - "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."
  - What exemptions* might apply?
    - Art. 9(2)(a) – explicit consent from employee
    - Art. 9(2)(b) – "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"
  - **GDPR empowers Member States to impose additional restrictions on processing of sensitive data.*

European Handbook on Equality Data

- Disclosure of diversity-related data must be voluntary
- Anonymous data should be processed where possible to improve voluntary participation of employee/applicant and reduce risk of misuse
- Anonymous data may not always serve diversity monitoring goals, necessitating the processing of personal data
- Employers may need to rely on consent as basis of processing where Member State laws exclude all other bases for processing
- Forms used to collect qualitative or quantitative information related to diversity should be concise, formulated in clear language, and tested before use

- "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."
- "Any employee being asked to provide data should be given a full explanation of the reasons for collecting the data, the importance of providing a response, how the data will be used and arrangements made for keeping the information secure and confidential."

– *European Handbook on Equality of Data, European Commission report, Dec. 2016*

Europe: Examples of National Law Rules

France

- More restrictive than GDPR; prohibits most collection of sensitive data
- Likely unable to store sensitive data about employees even if voluntarily provided
- Only anonymous surveys permissible
- Gender/citizenship may be collected only with consent from employee

Germany

- Some uses of sensitive data allowed in the employment context if used for workplace accommodations
- LGBTQ data subject to additional protections in the employment context
- Consent possible if it is for a positive opportunity in the employee's interest
- Some types of sensitive data may be collected only if done anonymously

United Kingdom

- Some uses of sensitive data allowed in the employment context if used for workplace accommodations
- LGBTQ data subject to additional protections in the employment context
- Consent possible if it is for a positive opportunity in the employee's interest
- Some types of sensitive data may be collected only if done anonymously

Processing Diversity Data: Common Challenges

- Non-legal cultural barriers: Even where an employer may legally engage in the collection of certain diversity data, cultural differences across multi-nationals could create friction with a U.S.-style diversity program.
    - Ex., French employers would not generally inquire about an employee's home life whereas U.S. employers encourage showing your differences at the office
- Validity of employee consent: Can employees "consent" to the provision of diversity information? If providing diversity information is necessary to receive an advantage due to a diversity characteristic, is consent "freely given"?
- More than just data protection: Restrictions to collecting diversity data arise outside of the data protection context. Labor laws, social security laws, etc. make it resource intensive to develop and implement a compliant diversity program.
- Different understanding of sensitive data: The types of data considered sensitive or with processing restrictions can vary across jurisdictions.

Processing Diversity Data – Best Practices

- Account for varying barriers processing restrictions at the national level
- Conduct a separate data protection impact assessment (DPIA) for each diversity program requiring the processing of data
- Provide clear notice to employees/applicants that the provision of sensitive data is optional and explain exactly how your company uses diversity data
- Restrict access to sensitive diversity data to only necessary individuals within your company
- For diversity metrics requiring identified data, aggregate data and discard record of individual's diversity classification
- If consent is the basis for collection, barriers allow employees to withdraw consent and inform them of that right
- Implement a written policy for treatment of diversity data and train relevant employees on how to follow the policy

Developing a D&I Program

What's your organization's strategy?

- Goals: What is your organization trying to accomplish? This will help guide advice and risk positions.
    - Different perspectives
    - Improved decision-making
    - Better alignment with customers/users
    - Ethics: the right thing to do
    - Larger talent pool (if resources are constrained)
    - Proactive effort to stem legal liability (for not being diverse)
- Stakeholders: Who are the key leaders to involve (e.g., CDO)? Who are the decision-makers?
- Responsibility: What teams, departments, or business units are responsible for implementing? What about ongoing management?

Developing a D&I Program

What's your organization's strategy?

- Legal Issues: Is privacy handling? HR? Both?
- Data: What data elements are you actually collecting?
  - Do you already have it or is it newly collected?
  - Limited to start with plans to expand or all at once?
  - Mandatory or optional?
- Global or Geo-specific approaches: Same approach across all countries? Collect more data in certain countries and less in others (e.g., U.S. v. EU)?
  - What if an applicant applies in both U.S. and EU?

Implementing a D&I Program

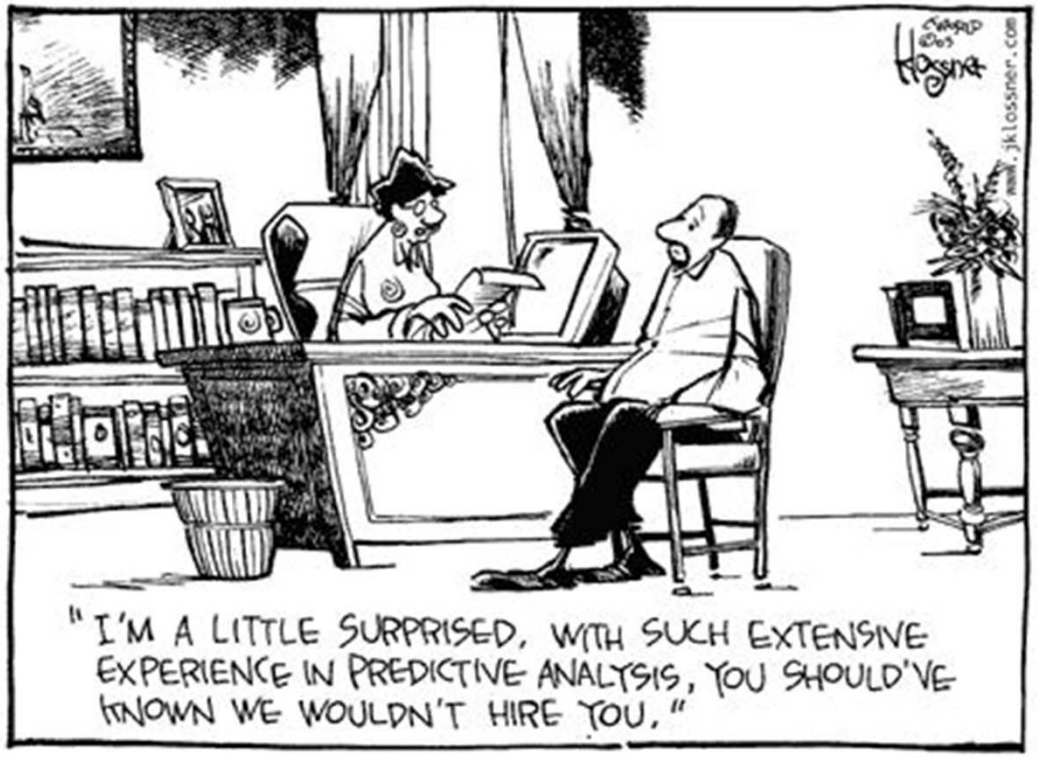
- Metrics: What metrics will be tracked to gauge success? Who is doing the tracking?
  - Are metrics internal only or to be reported externally?
- Privacy policies: What updates are needed to existing applicant and/or worker privacy policies, if any?
  - Is a new applicant privacy policy needed?
- Legal Basis: Are you using consent?
  - If so, who is collecting, tracking, and managing?
  - What is the process if someone revokes?
- Communications: What are we telling applicants and workers about the program? Who is responsible for communicating?
- Documentation and Training: Who is responsible for documentation and training related to the program?

Implementing a D&I Program

- Scope: What's the scope of implementation?
  - Pilot phase first?
  - Country by country or global roll-out?
  - Entire workforce or new hires?
- Inquiries: Who is responsible for handling inquiries about the diversity program?
- Evolution: Who is responsible for ongoing monitoring and management?
  - What about managing scope creep over time?

Data Analytics in the HR Space

A Day in the Life…



Data Analytics in the HR Space

A Day in the Life…

- How this data is captured, maintained, and used (key points in the ee lifecycle)
  - Talent system when applying
  - Onboarding
  - Ongoing ability to access/change through HR system
  - Specific company initiatives (e.g., pay equity)
- Data requests within the company (and maybe even from outside)
  - Men v. Women manager analysis: women better managers?
  - Employee networks: want to invite only those interested
  - Manager requests: want to build more inclusive/diverse teams

Processing Diversity Data: Common Challenges

- Recruiting teams want more data
  - What happens for those we don't hire?
  - Can we "deduce" race or sexual orientation status from social media?
  - What are our "data hygiene" practices?
- Data integrity: how "good" is the data?
  - Gender data: how many categories to include? What if people refuse?
  - Where are we getting the data?
  - Can company affinity groups be a proxy for race/ethnicity?
- Purposes for use:
  - Are we using the data to include or exclude?
- AI and Automated decisions: What can (and can't) we do with diversity data?
- Deletion requests:
  - What happens to the data set if someone requests deletion?
  - What's our approach for responding to these requests?

Watch for: Ever expanding scope

Processing Diversity Data – Balancing Act

- Innovate and Improve…But maintain clear access controls, data protections, manage for unintended consequences—and what about those internal security classifications
- Inform, educate, visibility…But beware “TMI”
- The power to evolve…but beware extremes and backlash

D&I Programs – Key Takeaways

- Transparency: Be transparent with your applicants and workforce about what data you are collecting and for what purposes
  - Avoid *"surprises"* that could impair your workforce's trust
- Stakeholder buy-in and alignment with company culture and values: have the right stakeholders from across the company be part of the initiative and the conversation
  - *Align initiative with company's culture and values*
  - *Clearly identify roles and responsibilities*
- Document your processes and protections: have a clear record of what your diversity data protection practices are, just in case

D&I Programs – Key Takeaways

- Be ready for tension between privacy and employment law issues: find the right balance for your organization
- Set clear goals: designate one or several clear “north star” objectives to guide program strategy and development
- How aggressive to be in the diversity program: some organizations push for more robust diversity programs (higher risk tolerance for privacy and employment law issues)
- Implementation process: consider phased roll-out and pilot programs
- Diversity and inclusion: don’t forget about inclusion efforts

Processing Diversity Data – Key Takeaways

- Access controls and data sharing controls: How widely should access to this data be granted; want to limit access to key "gatekeepers" due to sensitivity and potential for misuse
  - But need to balance controls with usability
- Anonymization can help: but when is something truly anonymized?
- Guardrails around use: set clear rules around how the company will use diversity data
  - Make sure ongoing use aligns with what you told the workforce
  - If use changes over time, change your messaging to align

Questions?

Parting words of wisdom

Thank You!