Data Management & Strategy Office

Handling Sensitive Personal Data

DATA POLICY

HAPPY DATA™

Introduction

This policy governs the process for collecting, accessing, using, storing, retaining, and disclosing sensitive demographic data. Our goal is to supply our teams and customers with the data needed to perform their duties and objectives while protecting the Demographic Data (defined below) from unapproved uses.

The company is legally required to share certain protected personal characteristics for government reporting purposes. However, for the collection and disclosure of information that we are not legally required to collect and disclose, individual participation is entirely voluntary. The company will only use and disclose Demographic Data in accordance with this policy. There will be no adverse impact on employment if a member of the company declines to provide any voluntary Demographic Data.

Definitions

Demographic Data—Demographic identification information of an individual's race, ethnicity, age, nationality, disability, gender, veteran status, citizenship, and data related to sexual preference and/or sexual orientation.

Disaggregated, Non-Anonymized Demographic Data—Demographic Data that is provided on an individualized basis or contains personally identifiable information.

Personally Identifiable Information (PII)—Data that can be used to identify a specific person.

Requestor—The individual(s) asking for permission to download, use, and store Disaggregated, Non-Anonymized Demographic Data.

Approver—The individual(s) granting or denying permission to download, use, and store Disaggregated, Non-Anonymized Demographic Data.

Data Governance Team ("DGT")—The team, led by the Data Governance Manager, comprising data governance personnel and activities at the company.

Denodo—The company's data virtualization platform. Denodo centralizes numerous data sources and makes them easily accessible.

DMS—The company's document management system.

Collibra—the company's data catalog, owned and maintained by the DGT.

Information Collected

As part of our diversity and inclusion initiatives, the company may collect certain data points that an individual voluntarily provides through a demographic data questionnaire in our human resources system. The information requested includes an individual's:

- Age
- Race and ethnicity
- Disability
- National origin
- Gender
- Sexual orientation
- Immigration status
- Veteran status

Some demographic information is required for benefit providers and legally mandated reporting. Outside of those characteristics, an individual's choice to provide Demographic Data is completely voluntary. They also may update their Demographic Data throughout their time at the company.

Individuals have a right to withdraw their consent and opt out of sharing their non-required, voluntarily disclosed Demographic Data at any time. Where data has already been provided to a third party and an individual wishes to withdraw their consent to its use, they should notify the DGT with the notice of withdrawing consent to sharing their Demographic Data.

How Demographic Data is Used

The company limits the processing of Demographic Data to the minimum necessary and only for specific permissible purposes. The company may use and disclose Aggregated and Non-Aggregated Demographic Data for:

- Diversity, Equity, and Inclusion objectives, such as analyzing the representation of historically underrepresented groups in the talent pipeline; assessing work opportunities, staffing and pitch teams; and determining ways to increase diversity in the talent pool and improve equitable outcomes.
- Evaluating and advancing the company's Diversity, Equity, and Inclusion initiatives.
- Developing marketing and recruiting materials reflecting the company's diverse population.
- Fulfilling our obligations under applicable laws, such as government diversity reporting.
- Demonstrating the company's diverse population to current and potential customers.

Sharing Data Externally

The company may share Aggregated Demographic Data on its website and in marketing and recruiting materials. In addition, the company may share Demographic Data externally with:

- Current clients who monitor the company's diversity efforts, otherwise benefit from the company's diversity efforts, and/or require Demographic Data for compliance with their outside counsel guidelines.
- Potential clients who request Demographic Data when assessing whether to engage the company.
- Service providers and other third parties who perform duties and functions on the company's behalf, such as employee survey companies or cloud service providers, which cannot use any identifying information for their own independent purposes.
- Governmental agencies, or pursuant to a subpoena, court order, or decree with appropriate safeguards where feasible to protect the integrity and confidentiality of Demographic Data.

Outside of the circumstances above, the company prohibits the sharing of Individualized, Non-Aggregated Demographic Data outside of the company.

How Demographic Data is Stored

The DGT must inventory and classify, or cause to be inventoried and classified, all Demographic Data collected by the company.

All datasets containing Disaggregated, Non-Anonymized Demographic Data must be formed using only data pulled directly from a system of record (a/k/a "source of truth") as determined and designated by the company.

Any datasets, reports, or other documentation containing Disaggregated, Non-Anonymized Demographic Data must be kept in the company's document management system (DMS) if downloaded from Denodo or the system of record. Storage outside of the DMS, including on a local drive or cloud storage accounts such as Teams, SharePoint, or OneNote, is prohibited.

How Demographic Data is Secured

All Demographic Data that is collected from individuals will be kept securely. The company follows these security measures to protect Demographic Data:

- All systems housing Demographic Data must pass an Information Security review that is reassessed on a regular basis to ensure any new vulnerabilities are found and patched.
- All reports or datasets containing Demographic Data that are required to be aggregated or anonymized must be properly anonymized or aggregated using statistical techniques, masking, or aggregated or displayed in a non-editable format (e.g., an image in a PowerPoint).
- All datasets containing Demographic Data must be vetted by the DGT prior to sharing to ensure they cannot be combined to form a single dataset that violates a provision in this policy.
- The DGT must keep, or cause to be kept, internal logs tracking which datasets have been "checked out" and by whom, as well as any relevant revocation period.

Requests for Demographic Data and Access Restrictions

Disaggregated, Non-Anonymized Demographic Data is only available upon request and approval by the DGT. Certain company personnel, by virtue of their role(s), have standing authority to access this data. A list of these roles was developed by the Diversity, Equity, & Inclusion Team. The DGT is responsible for ensuring the appropriate permissions are set in the data platform. Data requests may be approved in whole or in part.

Any requests for Demographic Data must be submitted to the DGT via email or via Request workflow in Collibra.

Where access to Disaggregated, Non-Anonymized Demographic Data is requested:

- The Requestor must describe a legitimate business reason for requesting the data.
- The Approver must conduct a Data Privacy Impact Assessment ("DPIA") prior to authorizing access. The Approver will deny access where the DPIA shows a risk level above a certain threshold.
- If access to Demographic Data is denied, the Approver will describe the reasons for the denial to the Requestor and propose alternative methods for meeting the Requestor's goals.

The individuals receiving access to Demographic Data must:

- Acknowledge that they have read this policy.
- Keep the dataset containing Demographic Data in a private folder on the DMS. The system will detect and delete the dataset from this folder on the 31st day after download. After deletion, the Requestor must request access again.
- Handle Demographic Data in accordance with the company's Data and Information Governance and Security Policies as found in the Company Manual.
- Only use Demographic Data for the purposes requested. If the scope of the request changes, the requestor must inform the DGT. If the new scope is not a logical outgrowth of the original request and does not comply with acceptable uses elsewhere in this policy, the request for expanded scope will be denied.

General Restrictions

No Demographic Data may be used in automated decision-making.

No company personnel, including an approved user, may print, or cause to be printed, physical copies of Disaggregated or Non-Anonymized Demographic Data.

No company personnel, including an approved user, may disseminate electronic or physical copies of Disaggregated or Non-Anonymized Demographic Data. This prohibition includes sending the data to an approved user's personal email address.

Retention of Demographic Data

The company retains aggregated Demographic Data as long as needed for our Diversity, Equity, and Inclusion initiatives and as legally required. Individual Demographic Data is retained for seven years post-employment.

Questions or Concerns

Any questions or concerns regarding this policy or the use of Demographic Data should be directed to the company's Data Governance Team.