denison™

DATA SECURITY

IT SECURITY AND GDPR COMPLIANCE

STRATEGIC ALIGNMENT

MERGER & ACQUISITION

TRANSFORMATION & TURNAROUND

TALENT MANAGEMENT

denisonconsulting.com

Table of Contents

Overview

Denison Consulting ("Denison") is a global consulting firm that specializes in organizational culture assessment and leadership development tools. Client organizations contract with Denison to administer and report on organizational culture surveys, leadership assessments such as "360" feedback reports, and to perform customized analytical work using data from these tools. Denison also offers consulting services around data results reviews and integration, facilitating "honest conversations", and action planning, as part of Denison's "Path to High Performance". In addition, Denison develops and maintains global databases that allow an individual client organization to compare its results against industry norms.

Denison serves clients in all industries around the world from its two offices in the United States and Switzerland. The Swiss office (Denison Consulting GmbH) manages the majority of Denison's business in the European Union and the European Free Trade Area (EFTA) (collectively, "Europe"). The U.S. office (Denison Consulting LLC) manages domestic and international projects for the rest of the world, which occasionally include European countries as well.

Justification for Receiving and Using Personally-Identifiable Information

Denison's business involves administering surveys and similar assessments within client organizations to measure organizational culture, leadership performance, and leadership development. The vast majority of data collected via these surveys and assessments are individuals' own opinions on a variety of subjects, voluntarily given in response standardized questions presented to all respondents. Individual responders may also provide non-standard verbatim feedback for many client projects.

For all organizational culture surveys and similar assessments, results are reported back to the client in aggregate, which generally does not require the use of personally-identifiable information (PII). However, Denison's clients often expect that results are also reported back at sub-organization levels, such as divisions or locations within an organization, or by some demographic information (e.g., gender, tenure at company, etc.). While such results are still aggregate in nature and not individual, the ability to segregate data into sub-organization levels requires having personally-identifiable information (PII) for most if not all respondents. For example, if the client organization wished to have separate reports for employees located in the United States, Australia, Japan, and Germany, information about the location of each employee would be necessary. The client instructs Denison which PII to collect, which then informs the report segments that are possible.

Obtaining this personally-identifiable information occurs one of two ways:

1. Most commonly, a client organization would provide PII directly to Denison via an HRIS file, with the necessary demographic and hierarchical information associated with each individual. Denison refers to this as a "data feed"; if one is used, it is typically provided to Denison in the early stages of a project. Having a data feed also allows for higher level of control over who can access the survey. Typically, this is done either by the creation of a uniquely-generated invitation link distributed by email (thus, requiring an email address and typically the name of the individual recipient), or through the use of some validation cross-check against known information about the intended respondent (e.g., an employee identification number). See also "How Data are Collected" on page 4.

2. If a data feed is not used, the only other option for collecting this information is voluntary disclosure by the employee respondent directly in the survey. This occurs by programming the requisite questions into the survey itself in an attempt to collect this information for reporting aggregated results back to the client. While this eliminates the need for handling a data feed from the client, this process is not as effective for reporting purposes because of the voluntary nature of answering such questions. For example, a question about an employee's location might be answered by, say, only 80% of respondents. For the 20% who did not answer the question, their responses would not be able to be classified or aggregated into any sub-organizational reports for the client. This approach also does not allow for the effective controls over who can access the survey.

For all leadership development and similar assessments (e.g., "360" evaluations), the principal deliverable to a client is an individual-level report, not reports in aggregate as with organizational surveys. By definition, the process of administering such assessments, and reporting their results to the client, requires Denison to receive personally identifiable information about the subject, including their name and a method of contacting them (typically an email address). In addition, some client organizations choose to pre-select other individuals who will be asked to evaluate the subject leader. In these cases, the client organization must provide same information about these other raters to Denison at the same time. Finally, in some cases, a client organization may also wish to receive aggregated or "composite" reports of several such subject leaders grouped together. The basis of grouping individuals will often be based on various hierarchical and demographic information about the individuals, in a manner similar to creating sub-organizational reports reports described above for organizational culture surveys.

In summary, the main purpose of any Denison survey or assessment is to collect the opinions of individual employees and represent them back to the client organization. While this does not entail the use of personally identifiable information per se, the practical reality is that PII is often required for survey access control, analysis, and reporting purposes in the vast majority of Denison's client engagements. Denison has no interest or business need for using PII beyond what is required for meeting immediate client obligations, except as noted under "Data Retained for Global Benchmarking" on page 8.

Types of Personal Data that Denison Collects and Uses

For client projects in which Denison collects personally-identifiable information (PII), that information is limited to only those elements that are necessary for the effective execution of a project, particularly data collection and reporting. Most typically, these data elements include:

- Employee Name
- (Unique) Employee Identification Number
- Employee email address
- Hierarchical information, such as an employee's division, location, and work unit within the organization
- Demographic information about the employee, commonly including gender/sex, job function or classification, and date of hire;
- Other PII that is deemed necessary for analysis and reporting as requested by the client organization and provided by the client to Denison for those express purposes.

• Denison does not usually collect sensitive PII, with the rare exception being when a client would like segment the results by race/ethnicity

See also "Information for Client Organizations" on page 8.

How Data are Collected

Denison surveys are conducted online via an SSL-encrypted website, using the same encryption technology used for secure banking transactions and online purchases. A survey can use one of the following general methods for collecting data:

Anonymous Link. The most common and most confidential way is via anonymous links. An anonymous link is a single link that can be sent to any number of participants either by Denison or by the client organization. Because the link is not specific to each individual, Denison cannot track which specific participants have taken the survey. This means that Denison would not be able to send reminders to only those users who have not completed the survey. Instead, all participants are reminded whether they have completed the survey or not.

Unique link. Denison can generate a unique survey link for each survey participant. The link is absolutely unique to that individual and should not be shared with others. This allows the ability to track survey participation and to send periodic reminders only to those participants who have not completed the survey.

Kiosk. For clients whose participants may share a computer terminal, Denison can issue a so-called "kiosk link". A kiosk link allows the survey to be completed by multiple participants at a single terminal. The downside of the kiosk link is that a participant is required to complete the survey in a single session and cannot partially complete a survey and return to it later.

Known Passwords. This hybrid approach combines many of the benefits of the methods described above. It uses a common invitation link that can be distributed either by Denison or internally by a client within that organization. "Validation" to take the survey occurs by asking the respondent to enter in a "known password" that corresponds to information included in the data feed that the respondent would know. The known password may be one variable in the data feed, or a combination of two or more variables. Common examples of "known passwords" include an employee ID number, a date of birth, an email address, or a combination of these or other variables.

Paper. We can also collect data through the use of paper surveys, for those instances where access to the Internet is limited or not available.

Where Data Are Stored

Virtually all data for all current and historical project work are stored in SQL databases on Denison-owned servers housed within secure, state-of-the-art data hosting centers that are monitored 24 hours per day, 7 days per week:

• Online Tech, near Ann Arbor, Michigan, USA (http://www.onlinetech.com). Generally, data from all projects run from Denison Consulting LLC are located here.

• Stadtwerke Konstanz GmbH, in Konstanz, Germany (https://www.stadtwerke-konstanzde). Generally, data from all projects run from Denison Consulting GmbH office are located here.

See also "Compliance with General Data Protection Regulation (GDPR)" on page 9.

Physical Security of Data

Physical access to Denison-owned servers located at both data centers in the U.S. and Germany is tightly restricted. Both offsite facilities are physically "hardened" with massive walls and ceilings, with limited and controlled physical access to storage rooms containing servers including the use of dual-door "mantrap" bays monitored both by cameras and by human staff through one-way mirrors, 24 hours per day, 7 days per week. Pre-designated, pre-approved two-factor authentication is required to gain physical access (typically a combination of a key pass and a biometric measure). Each data center maintains its own processes and protocols for managing records of who has physical access to each building. Only select Denison staff or their authorized designees have direct physical access these locations. A log is kept at each location of all visitors, who must be accompanied by an authorized individual. A list of Denison individuals having access to these facilities is maintained in each Denison office, respectively.

Data centers are staffed 24 hours per day, 7 days per week, 365 days a year, to monitor both security and operational functionality. The data centers are alarmed, climate-controlled, have redundant power backup systems, and chemical fire suppression systems. Each data centers' clients' assets (e.g., servers) are physically separated from each other in locked cages.

Virtual Security of Data

Denison systems employ network segmentation, hardened operating systems, firewalls, antivirus, malware protections, data leakage, intrusion detection systems, encryption protocols, and intrusion detection prevention.

Access to all Denison IT systems require employee-specific login credentials with passwords having high complexity (at least 11 characters, combination of letters and numbers, upper and lower cases, and at least one special character). Passwords are required to be changed every 30 days. Remote access to all data from outside of Denison's networks require a VPN with two-factor authentication.

There are no provisions for "sharing" accounts. Each individual employee has his or her own unique login that grants them access to data and applications stored on Denison's servers. There are no applications or systems within Denison's business that use common credentials for access to data.

When employees leave Denison, Denison IT is notified immediately and access and passwords are immediately terminated, and any physical equipment in possession of the former employee is captured.

As encrypted data are submitted during a client project, it is stored within a Microsoft SQL database located at one of the two data centers listed above. Denison's SQL databases are further encrypted using asymmetric encryption keys (a public key to encrypt the data and another private key to decrypt). Denison's SQL databases are clustered to guard against hardware failures, and to ensure the high availability of surveys and reporting data.

Denison has implemented comprehensive Disaster Recovery safeguards to protect against data loss or unscheduled downtime.

Functional Separation, Separability, and Pseudonymization

Denison maintains individual respondent-level results from multiple client projects in a sequel database, stored either on the U.S.- or German-

based servers described elsewhere in this document . The data base consists of numerous tables, each containing different data elements. Individual level results, including any personally-identifiable information, are associated with individual client projects, each one of which is stored in one or more tables within the database. Information identifying to which specific client project a case belongs is maintained in yet another separate table within the database, Access to individual-level results presently can be done only on a project-by-project basis. It is not technically possible to access multiple client projects' data simultaneously en masse.

Today, individual organizational culture survey projects that survey an organization's employees can in principle use pseudonymized data feeds. Individually-identifiable pieces of information such as employee names, identification numbers, e-mail addresses, and other specific information such as dates of birth or dates of hire can be omitted from a data feed or replaced with substitute variables such as matchback keys or grouped variables. However, a truly pseudonymized data feed would impose several limits on a typical project, most notably the inability to control access to a survey through a unique link or identity verification against other known variables in the data feed (see "How Data are Collected" on page 4.). Moreover, under no circumstance will Denison ever release identifiable individual-level results ("raw data") to a client, including when client-created pseudonymized "matchback" keys are present. This is done to preserve the anonymity of the respondent. If a client requests a copy of "raw data" from their project, it will be completely anonymized, preventing the client from having any ability to determine the identity of a specific respondent. (See also "Disposition of Data After Projects/Data Ownership" on page 7).

By definition, leadership assessment projects cannot be pseudonymized. The very purpose of such assessments is to receive and provide feedback about specific individuals by name.

Penetration Testing

Denison IT personnel manually regularly perform execute ongoing manual penetration tests to test for possible against our systems. In addition, current and potential clients from time to time notify Denison of their intention to perform penetration tests against databases and servers. Denison welcomes these opportunities to be tested, particularly when done in partnership to identify any potential weaknesses so that both Denison and its clients benefit from the discovery and correction of any issues.

Third-Party Data Storage

In addition to data stored on Denison-owned servers, a limited number of projects run on an external 3rd-party platform owned by Qualtrics, Inc., (Provo, Utah, USA). As an enterprise, Qualtrics attests to its own compliance to the European Union's General Data Protection Regulation (GDPR) and offers its clients (including Denison) the opportunity to specify the physical location of the server on which client project data are stored. These include servers (mostly through Amazon Web Services, who also publicly attest to their own compliance to GDPR) stored in the EU, including Germany and Ireland. There is also a Data Protection Agreement (DPA) in place between Qualtrics and Denison Consulting, GmbH.

All data on Qualtrics/AWS servers are limited to "leadership development" evaluation and assessment projects administered since September 2017 only.

Disposition of Data After Projects/Data Ownership

Denison will hold a client's data containing personally-identifiable information (PII) for as long as customer desires and/or return to client upon completion of project or destroy it and attest to its destruction to the client organization.

Raw data collected from employee respondents via surveys or assessments are the property of the client organization and are provided to the client organization upon request. However, in order to protect the identity and anonymity of the individual respondents, such data will not be returned with information that would explicitly allow the client to determine the identity of an individual employee's responses, or to know who has or has not completed the survey , .

Denison also reserves the right to retain anonymized data (i.e., without information that would allow an individual response to be directly identified) for purposes of further developing its global benchmark resources, as described below. In all such cases, retained data would be used only for analyses that aggregate multiple responses together.

Data Retained for Global Benchmarking

Denison has a limited business interest in maintaining de-identified demographic information to support specialized analysis for aggregated responses to its surveys and assessments, and to aid in ongoing research and development. A significant part of Denison's value to its client organizations is its large normative database of responses, against which a client organization's responses are typically compared. Typically, this is done most often at the organizational level. Occasionally, however, a client organization may request special analyses that require the the use of demographic information for isolating subsets of individual responses and comparing them against similar responses in the Denison database having a similar demographic profile. To meet these needs, Denison may occasionally run reports from original source projects, aggregate results using demographic information associated with individual-level responses collected at the project level. Any such analyses are always in aggregate, however, and not at an individual level.

Information for Client Organizations

Voluntary Participation

All of the Denison Surveys are voluntary and no one is ever required to participate. A participant may answer all, some, or none of the questions. Denison always keeps an individual's choice to participate (or not) strictly confidential and never discloses that information to a client organization. In some cases, a client organization may elect to make certain demographic questions required. In those cases, rather than disclose this information in response to required questions, a participant may elect not to finish the survey.

No Special Applications Are Required to be Installed in the Client's Environment

Clients often ask Denison to describe the applications that would be required to be installed in the client's environment, to attest to its security, and describe the type of support that Denison provides for such applications. These questions are inapplicable. Denison's survey and reporting platforms are independent of client systems and resources, with no software, network integration, or installation required. Survey access to the client via email delivery relying on authentication via secure link, using a combination of SurveyID and GUID

to guarantee security. However, there are minimal technical requirements necessary to ensure successful email delivery of survey invitations; see "Survey Requirements and Data Security Guide for Clients" below.

Survey Requirements and Data Security Guide for Clients

Denison has published online resources to help a client organization ensure that their technical environment is compliant with the minimum requirements for administering surveys and viewing reports online. These resources also describe in more detail how data is securely collected, stored, and used by Denison. For more information see: https://www.denisonconsulting.com/guides/datasecurity/

Data Privacy Consent Statement

Denison strongly recommends that its client organizations employ some form of data privacy consent statement to its employees who participate in a Denison survey or assessment. A typical example of such language is as follows:

"Your answers will have no impact on you as an employee or your privacy. If you are resident in a country with comprehensive data privacy laws, you have certain rights in relation to the information we collect. By responding to this survey, entering information and clicking the SUBMIT button, you are providing your consent."

"Denison Consulting understands your concern for privacy. The confidentiality and the anonymity of all survey takers (respondents) are of the utmost importance to Denison Consulting. In the event a particular data slice (report) would result in fewer than 3 applicable respondents , we never report against that demographic. No individually identifiable information will be used. Denison Consulting Consulting uses your e-mail address only to send invitation letters, send reminder letters and provide technical assistance to those taking the survey. Your e-mail address will not be used for any other purpose."

For additional examples of language that other clients have used, including for use within the European Union for General Data Protection Regulations (GDPR), see Appendix 1—Examples of Client Data Privacy Consent Statements on page 11.

Compliance with General Data Protection Regulation (GDPR)

Denison complies with the European Union's General Data Protection Regulation (GDPR). Up to the present time, Denison Consulting has been in full compliance with the provisions of the EU-US Data Privacy Shield, and before that, the International Safe Harbor Privacy Principles.

The majority of business in the EU (and European Free Trade Area, or EFTA) is managed from Denison Consulting GmbH ("Denison Europe") in Switzerland, where the managing director, Karl-Heinz Oehler, also serves as Denison's privacy officer for GDPR purposes. Denison Europe today handles all GDPR-related activities, including:

• Ensuring that Data Protection Agreements (DPAs) are in place between Denison and the client, allowing Denison to serve as a data processer; and

• Handling GDPR-covered data as part of a client project, according to the terms of the DPA

Denison US and Denison Europe also work collaboratively for trans-Atlantic projects requiring data collection both inside of Europe as well as outside. With a DPA in place, it is always the client's choice (as the data owner) as to whether to send GDPR-covered data

to either Denison Europe or Denison US for handling or processing. Most clients choose to keep such data inside of Europe, in which case the Denison Europe office will handle the data. Such projects are then co-managed from both offices, ensuring appropriate data separation at all times. (Denison US does not have access to any data, systems, or networks in Denison Europe.) At the completion of such projects, data from both locations can be anonymized and combined, allowing for global-level reporting while adhering to all GDPR requirements for the handling of Personally-Identifiable Information.

Denison trains and orients all personnel worldwide on GDPR and its requirements upon joining Denison, and thereafter again on at least an annual basis.

Appendices

Appendix 1—Examples of Client Data Privacy Consent Statements:

"We are pleased to invite you to participate in our 2019 Culture and Engagement survey conducted in collaboration with Denison Consulting.

Privacy Notice

"This survey is organized throughout [company], by [division] as controller and its subsidiaries and branch offices as co-controllers of the personal data that will be processed through the survey. Our lawful basis for the processing of the personal data is the controller's and co-controllers' legitimate interest to understand our workplace culture. Whether the common beliefs, values and behaviours we share at [company] are in the right place for where we are heading; and learn how we can improve that culture further going forward.

"The overall purpose of the survey for [company], and thus of the personal data processing that goes along with it, is to obtain anonymous responses of the participating employees. The suggestions will be used to improve our work climate and culture in which all of us are operating on a daily basis. Everyone will have the possibility to share their opinion from [date] to [date].

"The only recipient of your personal data is our processor Denison Consulting, which has contractually committed to [company] not to share personally identifiable data with the … organization. Personal data that will be processed by Denison Consulting are your name, e-mail address, and your feedback to the questions. The survey and the processing of the results are entirely anonymous, in that Denison Consulting shall share with [company] only anonymized feedback (elaborate using the feedback from Denison….).

"Denison Consulting is located in Michigan, U.S.A., with subsidiaries in Switzerland and the United Kingdom. When participating in the survey, your personal data will be transferred outside the European Union, to Denison Consulting's subsidiary in Switzerland, a third country for which the European Union has adopted an adequacy decision. The effect of such a decision is that personal data can flow from anywhere in the EU (and Norway, Liechtenstein and Iceland) to Switzerland without any further safeguard being necessary.

"Denison Consulting will retain your data no longer than required to provide the service to [company], and in any event have the personal data deleted by [date].

"You have the right to request from [company] access to, rectification or erasure of your personal data or restriction of processing, or the right to object to processing or have your personal data transferred to another party.

"For more information about the data processing in the Culture survey, or if you wish to exercise any of your rights explained above, you can reach out to [company's] Data Protection Lead, [name], [email].

"Participation in the Denison survey is voluntary, but we hope everyone will take the time to contribute to this important initiative. If you are participating in the Denison survey, you may answer all or some of the questions. Your answers will be used solely for the purpose stated in the survey advisory and will have no impact on you as an employee or your privacy."

FOR MORE INFORMATION

United States
121 W. Washington Street
Suite 201
Ann Arbor, MI, 48104
Phone: +1 (734) 302 4002

Europe
Freiestrasse 7
CH-8570 Weinfelden
Switzerland
Phone: +41 71 552 0571

United Kingdom
36 Coquet Terrace
Newcastle upon Tyne
Heaton, NE65LE England, UK
Phone: +44 7961 974 568