



## Data Security Information

DataPoints collects and maintains data provided by its users in the context of completing behavioral assessments (tests), surveys, and forms. This information includes contact information (first name, last name, email address), self-report information related to demographic characteristics (e.g., income, net worth, age), responses to our assessment questions, and scores on our assessments.

DataPoints does not maintain any type of client-related transactional or financial account-type information and does not currently integrate with platforms that maintain this type of data.

Our [privacy policy is located here](#). Our [terms of use are located here](#).

- 1) Assessment Platform
  - a) The site is built to professional development standards, using the Laravel framework.
  - b) The site is hosted at Amazon Web Services, with firewall protocols limiting server and database access. Amazon Web Services hosts our data. Here is the AWS Data Privacy policy overview: <https://aws.amazon.com/compliance/data-privacy-faq/>. AWS also applies the Amazon global data privacy terms. Those terms are described here: <https://www.amazon.com/gp/help/customer/display.html?nodeId=468496>.
  - c) Prior to launch, the DataPoints platform was subjected to a full, professional penetration test.
  - d) Our system includes firewalls configured to restrict access at each ingress / egress point on our network infrastructure.
- 2) Data Maintenance
  - a) Data is backed up daily, and the backup database is retained for 30 days. Therefore, data can be stored with the potential loss of only 24 hours worth of information.
  - b) DataPoints has both a primary and a secondary datacenter or cloud provider to support failover in the case of a business continuity planning (BCP) event.
- 3) Internal Data Policies
  - a) DataPoints has a small number of internal users with access to the platform and data.
  - b) When an employee or a contractor leaves the organization, their corporate accounts are deleted and all site access is revoked.
  - c) Data, including personal information, is periodically exported from the AWS platform onto personal work computers for purposes of statistical analyses by a limited number of high-level internal users.
- 4) Development
  - a) Product development is performed on the lower development and staging environment which does not contain production data.

- b) Access to the production database is granted on an as-needed basis for regular maintenance and support requests.

For questions about our data security and development, please contact [it@datapoints.com](mailto:it@datapoints.com).

--

DataPoints Security & Data Management Updated: January 2, 2022