Genos Data Security and Privacy Statement

Our general privacy policy can be found here:
http://www.genosinternational.com/privacy-policy

Genos International takes information security and individual privacy very seriously. As a provider of psychometric assessments and reporting services, we not only have a legal obligation but also an ethical obligation to maintain the privacy of individuals providing information to us.

To be clear, we will never provide an individual's raw data to third parties (not even to the employer themselves, even though they may be the entity paying for the assessments). The only exception is if an individual lodges a request for a copy of their own data, in which case we will provide it to them.

Genos International has developed an Information Security Management System in accordance with ISO27001:2013, a globally recognised standard for information security standards and controls. As such, we have taken numerous technical and operational steps to ensure the availability, integrity and confidentiality of all information that we store. Only permanent employees of Genos have access to Genos databases and only on an as-needs basis. Complex passwords are enforced, accounts are locked after multiple failed login attempts and security logs are reviewed on a daily basis.

Our production systems are hosted by Linode, LLC, a US company based in Galloway, NJ. Linode is one of the world's top hosting providers and is well known for its high reliability and proactive approach to infrastructure management. We utilise Virtual Private Servers hosted in Linode's Freemont and Atlanta data centres. Genos International Pty Ltd and Linode LCC have signed a Data Processing Agreement based on the EU Model Contract.

There are several layers of physical security at Linode's facilities. There are manned checkpoints and key card access required to get into the buildings. Once inside there are several layers of physical security before actually reaching the locked cages that house the servers, including biometric scanners, key cards and PIN numbers.

Each server instance is a fully virtualized instance of a physical machine. Each Xen instance runs its own kernel and user space in a dedicated segment of RAM limited to that instance. There are restrictions in place on the hosts to only allow Xen instances to access the disk images assigned to the account attached to it.

All communications with the production servers are encrypted, as are all backups. All servers are monitored 24x7 by both Linode and Genos and security patches are applied in a timely fashion. Firewall configurations are reviewed and firewalls tested monthly, as are all three backup systems. Staging servers with identical configurations are maintained so that patches and new software releases can be thoroughly testing before upgrading production systems.

Personal information such as names, email addresses, IP addresses and browser IDs that Genos collects when running emotional intelligence surveys are anonymised after five (5) years of dormancy. Additionally, individuals may request their personal data be anonymised at any time. Responses to questionnaires are retained indefinitely but are not attributable to individuals once their personal information has been anonymised. Data collected from demographics questionnaires is only ever analysed and reported on in the aggregate. These data sets are used for "norming" purposes as well as ongoing internal research to ensure the Genos survey instrument remains psychometrically reliable and valid.

We are proud of the fact that our production systems have experienced no unscheduled outages, data loss or data leakage due to attack, hardware failure or software failure since our very first online survey application was rolled out in April, 2004.

For more information about our privacy policy, please see:

https://genossurveys.com/privacy

Information on contacting Genos about privacy-related matters, including requests to have personal data anonymised, can be found at the bottom of that page.