Curious Thing Data Governance and Privacy Document

Curious Thing Pty Ltd (Curious Thing) is a Sydney-based conversational AI company for phone interviews. Curious Thing enables hiring managers to interview hundreds of candidates at once, giving all candidates a fair opportunity to shine through simple phone calls, and significantly reducing human biases from the CV-centric approach. We are also the winner of the Australiasian Talent Conference's 2019 Innovation award.

At Curious Thing, we understand the enormous potential and risks of data. We treat privacy and data security as the highest business priority. Curious Thing is committed to meeting the standards for privacy protection as outlined in the Privacy Act 1988 (Cth) and the Australian Privacy Principles (APPs).

What information do we collect from clients?

When creating a Curious Thing Hiring Manager account, we collect the hiring manager(s) name, email address and organisation name. They will be assigned a password that they can use to login to the Curious Thing client dashboard.

Password is one-way encrypted based on bcrypt.

What information do we collect from candidates?

When inviting a candidate for an AI interview, the client hiring manager(s) provides Curious Thing with the candidate's email address, name (or initials) and mobile phone number in the platform. This information is collected for candidate communication and authentication purposes.

The candidate will talk to Curious Thing's AI through a phone call. The AI will ask questions that the candidate will answer in a similar way to a regular human phone interview. Candidate answers (in audio) are recorded for analytics and benchmarking purposes.

Interview data storage

All data we collect is securely stored and processed within Australia (unless specifically required for clients outside Australia).

All interview data (e.g. interview recordings, interview analytics on candidate performance, and interview questions) is stored and backed up in Google Cloud Storage in encrypted, client-specific cilos provisioned in Sydney, Australia. Only the authenticated client admin(s) can access their candidates' interview data through the Curious Thing Admin Portal (https://admin.curiousthing.io/) during the contract period. All interview data stays on Australian soil and no data is piped offsite.

Data security governance

Curious Thing uses Google Cloud for cloud computing and cloud storage. All our clusters are provisioned in Australia so all data stays on Australian soil (unless specifically required for clients outside Australia). Interview data are securely stored in Google Cloud storage in client-specific buckets. Only client admin(s) can access their candidates' interview audio recordings and data through the Curious Thing Admin Portal (https://admin.curiousthing.io/). All service endpoints of Curious Thing are protected with HTTPS secured by a site-wide SSL certificate issued by a trusted certificate authority.

Google has one of the highest security standards in the cloud computing industry. Please refer to the following link for more details on Google Cloud's security and compliance:

https://cloud.google.com/security/
https://cloud.google.com/security/compliance/#/

Curious Thing uses AWS MariaDB for IAM (i.e., Identify and Access Management) from our AWS clusters, also provisioned in Sydney. It securely stores login credentials for client admins, as well as candidates when their interviews are created. Information we store on candidates is confined to their names and email addresses. No other personally identifiable information (PII) is retained on our platform.

Curious Thing uses IBM Cloud and Microsoft Azure for some of Curious Thing's interview analytics. Our IBM Cloud clusters and Azure clusters are again provisioned in Sydney to ensure data sovereignty. In addition, all cognitive APIs we use do not retain the payload (i.e., transcripts of the interview).

Data ownership

Our clients have final ownership of their interview data. Curious Thing retains the rights to use the interview data in a de-identified and aggregated fashion for its R&D and product improvement purposes.

Data retention

Upon contract lapse, the client admin login is revoked and they will lose access to their admin portal, which is the sole means to access the interview data (e.g., interview recordings and interview analytics on candidate performance). However, all interview data collected over the period is encrypted dumped from our production servers and is made downloadable through a secure link for a retention period of 30 days in a standard data dump format.

Other privacy requests

If you wish to make any further request about data privacy, please contact Han Xu, Chief Technology Officer han@curiousthing.io.

You should expect to have a response within 3 business days of making contact.