Data Privacy Policy
As Data Processor

Document Properties

Document History

Version	Description	Author	Date (dd/mm/yyyy)
1.0	Base Policy	Peter Stanbridge	25/05/2018

References

Title	Version	Author	Date (dd/mm/yyyy)

Stakeholders

Name	Role	Company
Peter Stanbridge	Technical Director	Cognitive Edge
Mark Anderson	Director	Cynefin Centre
Manami Majumdar	Programmer Team Leader	Cognitive Edge

Glossary

Term	Description

COGNITIVE EDGE DATA PROCESSES

Cognitive Edge (the “Company”) is committed to maintaining robust privacy protections for its users. Our Data Protection Policy and Procedures Document is designed to help you understand how we process, access and protect our client respondent data.

This Privacy Policy is specifically related to Cognitive Edge’s responsibility as a data Processor under the General Data Protection Regulation.

About Cognitive Edge’s Data Protection Policy and Procedures

Cognitive Edge has developed a “normal English” privacy policy to make the legal language of the policy understandable to all those who would visit the Cognitive Edge website or for use within client engagement contracts and staff/employee/contractor contracts. It does not intend to diminish the importance of the protection policy and procedures, just make them more accessible.

Main Procedure Policy

In the following:

- “The Client” refers to employees of the client who are authorised to request data access on the client’s behalf.
- “Client authorised person” is the authorised person mentioned in the previous bullet point.
- “Authorised person” refers to Cognitive Edge contractors, agents, affiliates engaged by Cognitive Edge to undertake certain technical and data management tasks.
- “Employee” refers to any employee of Cognitive Edge, including directors and managers.
- “Project respondent” refers to any person who has completed a signification of a fragment using the SenseMaker Collector software. It is the respondents data, which might include personally identifiable data, that is held on the Cognitive Edge system on behalf of the client.
- “Client data” refers to the respondent data collected using SenseMaker® Collector®

Data Processing Principles and Core Policies:

1. No employee or other authorised person shall gain access to any client respondent data without the written permission of a known client authorised person. Only requests from the known authorised persons shall provide permission to gain any access to such client data.
2. Employees or other authorised persons shall only gain access to that data required to undertake the requests given to us by the client. And they shall only perform the processing on that data as requested by the client. In order to gain access to data or projects, requestors will be required to provide proof of consent from the owner of the data, including a signature and specifically expressed purpose and intent. At the onset of a project, any authorized customer contacts and their information must be provided. These permissions apply to all users externally and all employees internally to Cognitive-Edge, including our technical team.
3. Under no circumstances will any client data be given to any third party. Any requests outside the client for client data will be handled via the client.
4. Under no circumstances will any client data be given to any employee or other authorised person other than for the purpose of undertaking required processing as requested by the client.
5. There will be times where a processing request will require client data to be downloaded to an employees local computer. This is particularly so if the software required to do the processing task is not available on the server. If the data processing request does require local processing, the standard technical procedures for client data access will be strictly followed and shall only be performed on local computers configured according to the standard Cognitive Edge local computer configuration and security requirements. In brief:
    a. Data shall be encrypted from source to local target.
    b. Connection to the server is to be accessed via VPN to AWS servers, and https to Singapore Servers, for the purposes of support desk access.
    c. Local computers should be password protected in accordance to Cognitive Edge password policy.
    d. Data decryption is to follow the safe Cognitive Edge procedure and utility (the decryption utility is only available to authorised computers).
    e. Local computer should not be left unattended with client data unless the computer disk is encrypted.
    f. Once processing has been completed, data is to be re-encrypted using the safe Cognitive Edge procedures and utility.

g. Data is to then be passed back to the server using a VPN connection for AWS servers and https for the Singapore servers, and https to Singapore Servers, for the purposes of support desk access.
h. Local data should be safe deleted immediately on completion. No client data is to be kept on any local computer at any time, except during the data processing task period.

6. All data access and processing is to be logged in the Respondent Data Process Log. The log contains information about the client and project, a reference to the authorisation, date/time and the names of the people who accessed the data and a description of the processing completed. This log is a by client log, and must be made available for client inspection on request by the client.
7. Any requests received by project respondents for any action on their data should initially be referred back to the client in order to receive their instruction to perform any data processing on that respondent's data. This point ensures the compliance of point 1 above.
8. Respondent data for completed projects (collection and analysis completed) will be deleted from the Cognitive Edge servers after the project analysis completion date unless the client has specifically instructed Cognitive Edge to keep it and that this request is agreed within the contractual terms of the client project engagement. Clients will be notified prior to project data removal and the client may request a password protected zipped copy of the full dataset as collected by the SenseMaker software.
9. An important class of data processing request is to anonymise or remove respondent data on request to the client from the respondent. These will be requested through the Anonymise Respondent Data Google form and all anonymisation and respondent personal data removal must be undertaken:
    a. Only on the request of the client. Direct requests from a respondent must be honoured but channelled via the client.
    b. Data anonymisation and removal is to be performed in strict accordance with the "Data Anonymisation and Removal" procedure guide. This guide explains how to perform both, and how to log and communicate back to the client/respondent that the task has been completed. All removal/anonymisation tasks will be checked by a second person to ensure correct completion.
10. Any request for data access by government bodies, regulators or any other such parties, is to be referred back to the client prior to any access or transfer of data to such parties. Under no circumstances is any respondent data to be passed to any third party, even regulators, without prior communication and permission from the client. Legalities over such party access to respondent data will be handled with the client prior to any data transfer.

Other Data Protection Procedures

The following additional points pertain to the protection and security procedures:

1. Each week, the application user access log will be examined to check any anomalies relating to user access to the SenseMaker system. The access to each client project will be compared to the access request log created by the “Request for Project Access” form filled in by the client when requesting user access to the system. Any anomalies will be reported within one working day to the client authorised person.
2. Each week, the network vault dashboard/report will be examined for any spurious access to the system. This will include, but not be limited to DOS attack attempts, repeated illegal login attempts, login attempts from suspicious regions and so on. Any anomaly impacting a client is to be reported to the client within one working day of discovery.
3. All employees and authorised persons agree to ongoing annual data security training and updates.
4. All employees and authorised persons shall not access any client data without having first signed a non-disclosure agreement that outlines the basic data security policies outlined in this document.

How We Use the Information

When respondents provide data via the SenseMaker Collection process, Cognitive Edge and the Cynefin Centre do not use or access the data in any way except for the purposes laid out above (any client requested data processing).

The only use of respondent data pertains to analysis as part of the SenseMaker data analytics and data export functions. These are only available to authorised client users.

Contact Us

If there you have a problem with the privacy policy, you can contact us by writing to privacy@cognitive-edge.com.