CLIENT DATA MANAGEMENT POLICY

Purpose

When a client's contract ends and they confirm they no longer need instant access to their site/data, they are provided with options for their site and data held by Cognisco.

They can choose to either archive, anonymise and archive or permanently delete their site and personal data.

(There are options to pay monthly for a read only site, data extracts per user extracted, data retention, or for a one-off export).

This policy provides an overview of the process used for the archiving and destruction of client records and personal data held by Cognisco, and to ensure that data is processed in line with the relevant legislation and codes of practice.

Data Archiving

Clients may purchase data archiving services from Cognisco.

Archived data is retained in the United Kingdom for the period of the data archiving agreement. All copies will be destroyed upon termination of the data archiving agreement.

Anonymised copies may be retained on other authorised Cognisco systems for the purpose of future operational use.

Process for Archiving

To archive data the following steps are to be followed:

1. Mark data as ready for archiving and add to the change control notice.
2. Circulate the change control notice for review and 'sign-off' agreement.
3. Perform export of SQL database to container in storage account.
4. Perform custom backup of App Service to container in storage account.
5. Verify backups exist in storage containers.
6. Retain storage container account.
7. Update the data retention schedule in the '**Data Control Records'** section of the Asset Register.

Data Destruction

Clients may purchase certificated data destruction service from Cognisco.

Process for Destruction

It is the responsibility of the client Lead Consultant to issue a notice to destroy data. The notice will be created as an internal support request case ticket on the corporate Support system. A copy of the notice will be sent to the manager of each department and the nominated salesperson.

To destroy data the following steps are to be followed:

1. Draw up a list of data items for deletion.
2. Create an anonymised copy of the data for retention and used by Cognisco.
3. Mark data for destruction and add to the change control notice.
4. Circulate the change control notice for review and 'sign-off' agreement.
5. Execute data destruction process:
    - Delete uptime tracking agent.
    - Delete blob (Media files/images) storage container.
    - Delete application service.
    - Delete traffic manager.
    - Delete DNS entries.
    - Delete database failover and redundancy configuration.
    - Delete database/tenant storage container.
    - Delete customer resource group.
    - Deprecate customer site release pipeline.

6. Attempt recovery by technical inspection and documented recovery techniques.
7. Verify destruction of data.
8. Record destruction event in the '**Data Control Records'** of the Assets Register.
9. Issue data destruction notification to client.

Disposal of Electronic Records and Media

The following table is not an exhaustive list of all possible media types, but instead offers a representative sample of the most common forms of media currently in use. These media types also demonstrate the characteristics that determine the appropriate deletion or destruction methods required to assure data is non-retrievable.

Media Type	Data Storage Mechanism	Suggested Removal Methods
Hard Disk Drives	Non-volatile magnetic	Pattern wiping, Incineration
CDROM/DVD-R	Write once optical	Abrasion, Incineration
CD-RW/DVD-RW	Write many optical	Abrasion, Incineration
Magnetic Tape	Non-volatile magnetic	Degaussing, Incineration
Flash Disk Drives	Solid state	Pattern wiping, Physical destruction
Paper Based	Locked cabinet	Shredding, Incineration

Removal of Data from Site and Remote Access

Client data will not be removed from site except in exceptional circumstances and only with the written permission of the Data Protection Officer and the client.
The Domain Administrators, as agreed by the Data Protection Officer, will be allowed remote access. The list of Domain Administrators will be reviewed every 3 months by the Data Protection Officer.
Remote working may be permitted in exceptional circumstances for other employees, but only after consultation with the client and written authorisation from the Data Protection Officer.

Anonymous Data

On occasions Cognisco may be permitted to retain a version of a client's assessment results which have been made anonymous. This means that no data can be identified as belonging to any specific individual/employee.

Developers using local copies of data must ensure that the data has been processed and is anonymous.

It must not be possible to identify the organisation or any individual by combining separate pieces of information held by Cognisco.

All references to identifiable data must be replaced with a 'type' or randomised name. For example, the client's name should be changed to 'UK International Bank 2'. A Job Title must be changed to remove specific references e.g. "Head of Retail Banking (HBSC)" would change to just "Director" or "Head of Department".

The following information data should be subject to this process if the client has agreed in writing to the process:

- Organisation Name
- Project Name
- Programme Name
- Module Name
- Topic Name
- Question Stem/Response
- User Login Name, Password, First Name, Surname, Job Title
- Group Names
- Database Name
- Network Folder Name

Following the process to ensure all retained data is anonymous, and the destruction of all other data is completed an audit will be undertaken by a trained member of staff.

Additional options

Clients may purchase the following services from Cognisco, where available:

Read only service

Cognisco will retain a read only version of MyKnow for a single user account to access the system on a read only basis.

Data Export

Cognisco will provide a onetime data export of all user, assessment and competency data as a set of csv files on request from the client.

Data Retention

Cognisco will undertake to retain a non-operational copy of assessment, competency and/or training data on its MyKnow system. This will allow you to utilise this information for future decisions, training requirements or for auditing purposes. Data will be encrypted and stored in our UK Microsoft Azure Cloud Service.

Data Extracts

For retained data, Cognisco will supply data extracts on request, the options are:

1. Extract report creation (in a format to be agreed) of the relevant information stored in the system on an employee basis.

2. Extract request - To provide an extract we will retrieve the data from storage, resurrect the database in a readable form and then run the extract report for the given users and then decommission the temporary environment.

Date of Review: 20.03.2024	Signed: *A Ellis*
Date of Next Review: Jan 2025	Print Name: Angela Ellis ISMS Manager