CLIENT DATA MANAGEMENT POLICY

Purpose

This policy provides an overview of how Cognisco collects, stores, protects, uses and disposes of client information.

It provides details of data options and the processes used for the disposal of client records and personal data held by Cognisco - to ensure that data is processed in compliance with relevant regulations, controls and codes of practice.

Data Collection and Storage

Client data is sent to the helpdesk via Freshdesk
Client data is hosted, processed and stored in Azure Cloud (UK).
All assets are within Azure Cloud.
Client data is stored for the performance of a contract and within the timeframe of the contract/data agreement.
Client data is removed when the timeframe expires i.e. the contract / data agreement ends.

Data Security

Client data is protected from unauthorised access, loss, or misuse using encryption, access controls, and regular security audits.

Cognisco has an Incident Management Plan (IMP) and a Business Continuity and Disaster Plan (BCP).

Data Usage and Sharing

Data used for business purposes is employee name, email address Depending on requirement this may extend for example: location, grade, role.
Data is not shared with third parties.

Data Governance

There are established procedures for maintaining client information, and a framework for managing data assets - including roles, responsibilities and quality standards.

Compliance

Applicable controls: ISO27001:2022, ISO9001:2015, Cyber Essentials
Cognisco Information Security Management System (ISMS)

Adherence to relevant data protection laws and regulations:
The Data Protection Act 1998
The General Data Protection Regulation (GDPR) 2018
Cognisco data policies.

Data Disposal

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

The client should advise Cognisco within **ten-days** of their requirements for the disposal of their personal data.

If no instructions are received from the client - then all client access will be turned-off and the account will be closed down.

We will retain the data for a further **30-days** after which, if we have still received no instructions from the client - all personal data will be anonymised and will be irretrievable. We will inform the client that their personal data has been removed from our system.

Data Options

There are options to pay for data archiving, a read-only site or for a certified full data destruction service.

Data Archiving

Archived data will be 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, and a certificate will be provided verifying the completion of this activity.

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

Read-Only Service

Cognisco will retain a read-only version of the system - including the MyKnow application for a single user account to access the system on a read-only basis.
Data will be retained in the United Kingdom for the period of the agreement. All data will be destroyed when the contract agreement ends, and a certificate will be provided verifying the completion of this activity.

Data Destruction

Clients may purchase a **certificated** data destruction service from Cognisco.

Cognisco will securely and irretrievably destroy all data identifiable as relating to your organisation. A certificate will be provided verifying the completion of this activity.

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.

Date of Review: 07.08.2025	Signed: A Ellis
Date of Next Review: Jan 2026	Print Name: Angela Ellis ISMS Manager