Data Protection & Data Retention Policy

Context and overview

Introduction

Cluas Centre Ltd needs to gather and use certain information about individuals. These can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact. This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards - and to comply with the law.

Why this policy exists

This data protection policy ensures Cluas Centre Ltd :

- Complies with data protection law and follows good practice
- Protects the rights of staff, customers and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Data protection law

The Data Protection Act 1998 describes how organisations - including Cluas Centre Ltd - must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically, on paper or on other materials. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.
The Data Protection Act is underpinned by eight important principles. These say that personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not be held for any longer than necessary
6. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways

8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

People, risks and responsibilities

Policy scope

This policy applies to:

- The head office of Cluas Centre Ltd
- All staff and volunteers of Cluas Centre Ltd
- All contractors, suppliers and other people working on behalf of Cluas Centre Ltd

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- ...plus any other information relating to individuals

Data protection risks

This policy helps to protect Cluas Centre Ltd from some very real data security risks, including:

- Breaches of confidentiality. For instance, information being given out inappropriately.
- Failing to offer choice. For instance, all individuals should be free to choose how
- the company uses data relating to them.
- Reputational damage. For instance, the company could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with Cluas Centre Ltd has some responsibility for ensuring data is collected, stored and handled appropriately. Each individual that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles. The board of directors is ultimately responsible for ensuring that Cluas Centre Ltd meets its legal obligations.

General staff guidelines

- The only people able to access data covered by this policy should be those who need it for their work.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, strong passwords must be used and they should never be shared.
- Personal data should not be disclosed to unauthorised people, either within the company or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.

Data storage

These rules describe how and where data should be safely stored. When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it. These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer.
- Data printouts should be shredded and disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be protected by strong passwords that are changed regularly and never shared between employees.
- If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing services.
- Servers containing personal data should be sited in a secure location, away from general office space.
- Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures.
- Data should never be saved directly to laptops or other mobile devices like tablets or smartphones.

- All servers and computers containing data should be protected by approved security software and a firewall.

Data use

Personal data is of no value to Cluas Centre Ltd unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure.
- Data must be encrypted before being transferred electronically.
- Personal data should never be transferred outside of the European Economic Area.
- Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.

Data accuracy

The law requires Cluas Centre Ltd to take reasonable steps to ensure data is kept accurate and up to date. It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.
- Cluas Centre Ltd will make it easy for data subjects to update the information Cluas Centre Ltd holds about them. For instance, by sending an email or in person.
- Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.

Subject access requests

All individuals who are the subject of personal data held by Cluas Centre Ltd are entitled to:

- Ask what information the company holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how the company is meeting its data protection obligations.

If an individual contacts the company requesting this information, this is called a subject access request. Subject access requests from individuals should be made by email; contact@cluas.ie. The data controller will always verify the identity of anyone making a subject access request before handing over any information.

Providing information over the telephone

Any employee dealing with telephone enquiries should be careful about disclosing any personal information held by Cluas Centre Ltd over the phone. In particular the employee should:

- Check the identity of the caller to ensure that information is only given to a person who is entitled to that information,
- Suggest that the caller puts their request in writing if the employee is not sure about the identity of the caller and in circumstances where the caller cannot be verified.

Cluas Centre Ltd. can and will only provide personal information to the parent/guardian of the child or to the client when over 18 years of age. Only parents/guardians or adult clients over 18 can request personal information to be forwarded or discussed with a third party.

Disclosing data for other reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject. Under these circumstances, Cluas Centre Ltd will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

Data Retention Policy

Cluas Centre Ltd must comply with the provisions of section 2(1)(c) of the Data Protection Acts 1988 and 2003. The Acts set out the principle that personal data shall not be kept for longer than is necessary for the purpose or purposes for which it was obtained.

All retained records containing personal data will be stored safely, securely in such a way as to preserve its privacy and confidentiality.

Access to personal data will be restricted to those who reasonably require it in order to perform their work within Cluas Centre Ltd. Personal Data will not be shared with other persons except in connection with their clinical management and treatment, other than by the expressed consent of the client. Cluas Centre Ltd will not share retained personal data with third parties for advertising or marketing/ promotion purposes.

Clinical Data: Physical and electronic records of clinical data is deleted/ confidentially destroyed after 6 years from last meeting (usually the final review).

Financial Data: Financial Data is kept for 6 years to adhere to revenue guidelines. Financial Data (including non-payment of bills) can be given to Irish revenue at revenue's request.

Contact Data: Contact Data is kept for 6 years to allow processing of Financial Data if required. This may be retained for longer to for safety, legal request, or child protection reasons.

Record type	Default retention period	Final disposition
Client files	Retain for 6 years from the final review meeting (at discharge).	Shredding / secure deleting of electronic records
General email correspondence - client or lead related	Retain for 2 years, or until they cease to be of administrative use	Appraise and evaluate for archiving where relevant otherwise, secure deleting of electronic records
General correspondence	Retain for current year,	Appraise and evaluate

including emails - not client related	or until they cease to be of administrative use	for archiving where relevant otherwise, secure deleting of electronic records
Accounts related data	Retain for current year plus 6 years and accountant audit signed off	Shredding / secure deleting of electronic records
Payroll	Retain on personnel file for duration of employment and for 5 years after last pension payment	Shredding / secure deleting of electronic records
Personnel files	Retain on personnel file for duration of employment and for 5 years after last pension payment	Shredding / secure deleting of electronic records
Written HR related allegations & complaints (incl ex employees)	Retain indefinitely	Appropriate filing / archiving
Insurance Policies	Retain for 7 years	Shredding / secure deleting of electronic records