Data Protection Policy

For the attention of:	Staff, Management and Board
Date reviewed:	May 2018
Date of next review:	May 2019
Revision no:	Version 3
Approved by:	Board of Directors
Document owner:	Head of Legal Services

1.0 Introduction

Everyone has rights with regard to how their personal data is handled. This Policy sets out the obligations of Clúid Housing ("Clúid") under data protection law and how that commitment is carried out with regards to the collection and use of personal data. Data protection law safeguards the privacy rights of individuals as well as laying down responsibilities for the processing of personal data. Data protection law imposes restrictions on how Clúid may collect and process that data.

It is intended that by complying with these guidelines, Clúid will adhere to best practice under data protection law.

2.0 Purpose

Clúid must comply with the data protection principles set out in the General Data Protection Regulation (GDPR)[1] . The Policy sets out the rules and the legal conditions that must be satisfied in relation to the collecting, obtaining, handling, processing, storage, transportation and destruction of personal data.

3.0 Scope

The Policy applies to all personal data and sensitive data collected, processed and stored by Clúid in relation to its employees, service providers and tenants ("**Data Subjects**") in the course of its day to day activities. Data can be held by Clúid in paper form or electronic form.

The Policy applies to all members of staff, including contractors and temporary personnel, who process personal data as part of their work. Clúid treats the rights of all data subjects equally, whether they are employees, tenants or suppliers.

4.0 Definition of Data Protection Terms

Data is information which is stored electronically, on a computer, or in paper files. This includes IT systems and CCTV systems.

Data Subjects include all living persons about whom Clúid holds personal data.

Personal data means data relating to a living person who is or can be identified, either from the data or from the data in conjunction with other information that Clúid holds as a Data Controller. Personal data can be simple facts (such as a name, address or date of birth) or it can be an opinion (such as a staff performance review).

Data Controller is the individual or organisation who controls and is responsible for the keeping and use of data. Clúid is a Data Controller.

[1] *The General Data Protection Regulation (GDPR) will come into force on the 25th May 2018, replacing the existing data protection framework under the EU Data Protection Directive. Ireland will introduce a new Data Protection Act later in 2018 to repeal & replace the existing data protection acts.*

Data users include employees whose work involves using personal data. Data users have a duty to protect the information they handle by following the Policy at all times.

Processing means doing anything with the data. There is a long list of examples of processing set out in GDPR. Some examples include collecting, recording or keeping data, using the data or destroying the data.

Sensitive personal data includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health, sexual life, criminal convictions or the alleged commission of an offence. Sensitive personal data can only be processed under strict conditions, and usually requires the consent of that person in order to process it.

5.0 Data Protection Principles

Clúid staff must deal with all personal data in a responsible manner and in accordance with the following eight data protection principles which state that data must be

1. Obtained and processed fairly
2. Used only for the purpose that it was gathered in the first instance
3. Kept safe and secure
4. Accurate and up to date
5. Disclosed only in line with the original purpose
6. Not excessive but relevant and adequate
7. Retained only for as long as needed for the original purpose
8. Presented to data subjects on request

Source: Data Protection Commissioner https://www.dataprotection.ie

6.0 How are the data protection principles applied at Clúid?

In the course of its daily organisational activities, Clúid acquires, controls, processes and stores personal data of data subjects. Data protection law imposes restrictions on how Clúid may collect and process that data. When gathering personal data Clúid must state its reasons for looking for it, what it will be used for and who it will be shared with. Clúid must ensure that any data collected is limited to what it actually needs, for purposes which are specific, lawful and clearly stated.

Before Clúid processes any personal data it must tell data subjects that they have a right to complain if they are unhappy with the reasons for processing and what rights they have under GDPR. Clúid must ensure that it uses technical measures and has procedures in place to secure the personal data against unauthorised access, unlawful process or accidental loss or damage.

Where possible, Clúid will seek the consent of the data subject before their data is processed. Where it is not possible to seek consent, Clúid will ensure that collection of the data is justified under one of the other lawful processing conditions set out under GDPR, for example, legal obligation, for a contract etc.

Clúid, as a landlord, collects personal data to create a tenancy agreement with a tenant, for example, name, address, contact information, gender, family relationships, date of birth. Clúid can process tenants' bank details or credit card details where relevant for tenants to make payments. Clúid processes the personal data of tenants so that it can manage the tenancy, for example, liaising with tenant for payment of rent, organising repairs, dealing with tenant issues or complaints etc.

Clúid also keeps details of phone calls and logs of phone calls, email correspondence and paper correspondence. If a person makes a complaint Clúid will process the details of that complaint.

Clúid, as an employer, collects personal data of its staff to create an employment contract. Clúid processes the personal data of staff in order to pay wages, and maintain a personnel file etc.

Access to and management of staff and tenant records is limited to those staff members who have appropriate authorisation.

Clúid must also comply with statutory obligations and under some laws Clúid can be obliged to share personal data of data subjects, for example, to the Residential Tenancies Board to register a tenancy, or to An Garda Siochána where a crime has been committed.

Where Clúid intends to record activity on CCTV, a notice will be posted in full view. For further details on the use of CCTV, see Clúid's CCTV policy.

If a person visits Clúid's website to browse, read or download information Clúid automatically collects and stores information about the use of the website through certain cookies that are set. Please refer to Clúid's Cookies Policy and Privacy Policy. This can be found on the website at www.cluid.ie/privacy-policy

7.0 What obligations must Clúid staff members comply with?

1.1. Keep confidential

All Clúid staff must keep confidential any personal data they are using as part of their employment. Not all staff members are expected to be experts in data protection law. However, Clúid is committed to ensuring that its staff are sufficiently aware of the data protection law in order to be able to anticipate and identify a data protection issue, should one arise.

1.2. Mandatory training

Clúid has provided data protection awareness training to all staff members which provides staff with the ability to recognise, report and address potential data breaches and to respond to subject access requests efficiently. Staff have been trained to ensure that where personal data must be shared with suppliers that Clúid will only use suppliers who have robust data protection policies in place (See **Third Party Processors** below).

1.3 Keep data accurate

Clúid is obliged to keep personal data accurate and up to date. Clúid must correct information which is inaccurate or misleading. Clúid must take steps to check the accuracy of any personal data when it is being collected and at regular intervals afterwards. Inaccurate or out-of-date data should be destroyed.

1.4 Notify of changes

Staff members should ensure that they notify their manager/Human Resources of any relevant changes to their personal information so that it can be updated and maintained accurately, for example, a change of address.

1.5 Keep for only as long as necessary

Personal data should not be kept longer than is necessary for the purpose for which we collected it. For guidance in relation to data retention policies staff members should contact their manager. This means that the retention period for personal data will vary depending on the type of personal data and the reason it was collected. Clúid has various regulatory and legal obligations to keep certain data for a specified period of time. Clúid will conduct regular assessments in order to establish the need to keep certain personal data. Where it is no longer required to be kept Clúid will destroy, erase or otherwise put this data beyond use.

8.0 How can staff members ensure that data is kept safe?

Staff members must ensure that data is kept safe by:

1. Ensuring desks and cupboards are kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)
2. When destroying information paper documents should be shredded. Floppy disks and CD-ROMs should be physically destroyed when they are no longer required.
3. Data users should ensure that individual monitors do not show confidential information to passers-by and that they lock or log off from their PC when it is left unattended.

9.0 Providing information over the phone

Any staff member dealing with telephone enquiries should be careful about disclosing any personal data held by Clúid over the phone. In particular the employee should:

1. Check the identity of the caller to ensure sure that information is only given to a person who is entitled to that information.
2. Suggest that the caller put their request in writing if the staff member is not sure about the identity of the caller and in circumstances where the identity of the caller cannot be verified.
3. Refer the request to their manager for assistance in difficult situations. No staff member should feel forced into disclosing personal information
4. Where applicable, advise that the call is being recorded in accordance with the Call Recording Policy.

10.0 How does Clúid manage personal data queries?

Clúid has set up a Data Protection Working Group ("DPWG") to handle and respond to all personal data queries. The DPWG is led by the Data Protection Coordinator who is also responsible for monitoring and continually improving internal data protection processes. The Data Protection Co-ordinator can be contacted by telephone (01 7072088) or by emailing dataprotection@cluid.ie

11.0 Subject Access Requests

If a data subject requests a copy of their personal data, this is known as a Subject Access Request. Clúid has a Subject Access Request Policy which it must comply with to deal with all requests. The request does not have to be in writing. However, the request must be accompanied by required proof of identity and address. All requests will be processed in a timely manner and within not more than 30 days from the receipt of the request or in accordance with the legislation. For ease of convenience, we have created a Subject Access Request form to assist data subjects in making a request. It can be a useful checklist as to what information is required from the data subject when making a request. A copy of the Subject Data Request form is available on the company website https://www.cluid.ie/data-protection.

12.0 Third Party Processors

As Clúid controls and is responsible for keeping and using personal data on its computers or in manual files, it is known as a Data Controller. This means Clúid has obligations under data protection law to keep the data safe. As part of its day to day business activities Clúid engages trusted third parties to carry out work on its behalf. Some of these third parties must hold or process the personal data to perform their job. These third parties are known as Data Processors. To ensure that all personal data that is held or processed by Data Processors is kept safe, a written agreement is entered into with the Data Processor, which sets out their obligations to Clúid. It sets out the specific purpose or purposes for which they are engaged, and the understanding that they will process the personal data in compliance with data protection law.

13.0 Data Breaches

It is important that all staff are aware to whom they should report such a breach. Staff need to be made fully aware as to what constitutes a breach. Clúid has a Data Breach Policy in place and this forms part of staff awareness training.

Having such a procedure in place will allow staff to recognise a breach or a potential breach early on so that it can be dealt with in the most appropriate manner

Details of a data breach should be recorded accurately, including the date and time the breach occurred, the date and time it was detected, who/what reported the breach, description of the breach. For further information, see the Data Breach Policy.

14.0 Enforcement

The Policy applies to all employees of Clúid. It also applies to contractors and temporary personnel of Clúid.

Adherence to the Policy is overseen by the line managers. If an employee considers that the Policy has not been followed in respect of personal data about themselves or others they should raise the matter with their line manager as soon as possible.

The Data Protection Co-ordinator will monitor any breaches of the Policy and will work in tandem with the line manager to ensure ongoing general compliance. Data protection training is mandatory for all employees and training will be continually offered for employees.

Any breach of the Policy will be taken seriously and depending on the severity and nature of the breach may result in disciplinary action up to and including dismissal. Clúid reserves the right to take such action as it deems appropriate against any data users who breach the conditions of this policy.

15.0 Review of Policy

Clúid will continue to review the effectiveness of the Policy to ensure it is achieving its stated objectives on at least an annual basis and more frequently if required taking into account changes in the law and organisational or security changes.

16.0 References

For further information relating to data protection please refer to:

- Clúid's Subject Access Request Form
- Clúid's Data Breach Policy
- Clúid's CCTV Policy
- Clúid's Website Privacy Policy
- Data Protection Commissioner's Website https://www.dataprotection.ie