Casadh CLG Data Protection Policy

Introduction

The purpose of this document is to provide a concise policy statement regarding the Data Protection obligations of Casadh CLG This includes obligations in dealing with personal data, in order to ensure that the organisation complies with the requirements of the relevant Irish legislation, namely the Irish Data Protection Act (1988), and the Irish Data Protection (Amendment) Act (2003).

Rationale

Casadh CLG must comply with the Data Protection principles set out in the relevant legislation. This Policy applies to all Personal Data collected, processed and stored by Casadh CLG in relation to its staff, service providers and clients in the course of its activities. Casadh CLG makes no distinction between the rights of Data Subjects who are employees, and those who are not. All are treated equally under this Policy.

Scope

The policy covers both personal and sensitive personal data held in relation to data subjects by Casadh CLG . The policy applies equally to personal data held in manual and automated form (ECASS & ILP Databases).

All Personal and Sensitive Personal Data will be treated with equal care by Casadh CLG Both categories will be equally referred-to as Personal Data in this policy, unless specifically stated otherwise.

This policy should be read in conjunction with the associated Subject Access Request procedure, the Data Retention and Destruction Policy, the Data Retention Periods List and the Data Loss Notification procedure.

Casadh CLG as a Data Controller

In the course of its daily organisational activities, Casadh CLG acquires, processes and stores personal data in relation to:

1. Full Time Employees of Casadh CLG
2. Participants of Casadh CLG
3. Customers of Casadh CLG
4. Volunteers working with Casadh CLG either in a Therapeutic or Management capacity
5. Programme Sponsors, The Department of Social Protection and The Health service Executive via the Local (South Inner City) Drugs & Alcohol Task force
6. Third party service providers engaged by Casadh CLG where client personal information may be discussed

In accordance with the Irish Data Protection legislation, this data must be acquired and managed fairly. Not all staff members will be expected to be experts in Data Protection legislation. However, Casadh CLG is committed to ensuring that its staff have sufficient awareness of the legislation in order to be able to anticipate and identify a Data Protection issue, should one arise. In such circumstances, staff must ensure that the Data Protection Officer is informed, and in order that appropriate corrective action is taken.

Due to the nature of the services provided by Casadh CLG , there is regular and active exchange of personal data between Casadh CLG and its Data Subjects. In addition, Casadh CLG exchanges personal data with Data Processors on the Data Subjects' behalf.

This is consistent with Casadh CLG 's obligations under the terms of its contract with its Data Processors.

This policy provides the guidelines for this exchange of information, as well as the procedure to follow in the event that a [Company] staff member is unsure whether such data can be disclosed.

In general terms, the staff member should consult with the Data Protection Officer to seek clarification.

Subject Access Requests

Any formal, written request by a Data Subject for a copy of their personal data (a Subject Access Request) will be referred, as soon as possible, to the Data Protection Officer, and will be processed as soon as possible.

It is intended that by complying with these guidelines, Casadh CLG will adhere to best practice regarding the applicable Data Protection legislation.

Third-Party processors

In the course of its role as Data Controller, Casadh CLG engages a number of Data Processors to process Personal Data on its behalf. In each case, a formal, written contract is in place with the Processor, outlining their obligations in relation to the Personal Data, the specific purpose or purposes for which they are engaged, and the understanding that they will process the data in compliance with the Irish Data Protection legislation.

These Data Processors include:

- Care and Case Management Workers (Project Workers, Project Supervisors and Administration Staff.

Our Commitment

Casadh CLG is committed to ensuring the security and protection of the personal information that we process, and to provide a compliant and consistent approach to data protection. We have always had a robust and effective data protection program in place which complies with existing law and abides by the data protection principles. However, we recognise our obligations in updating and expanding this program to meet the demands of the GDPR and the

Casadh CLG are dedicated to safeguarding the personal information under our remit and in developing a data protection regime that is effective, fit for purpose and demonstrates an understanding of, and appreciation for the new Regulation. Our preparation and objectives for GDPR compliance have been summarised in this statement and include the development and implementation of new data protection roles, policies, procedures, controls and measures to ensure maximum and ongoing compliance.

How We are Preparing for the GDPR

Casadh CLG already have a consistent level of data protection and security across our organisation, however it is our aim to be fully compliant with the GDPR by 25th May 2018.
Our preparation includes: -

- ***Information Audit*** - carrying out a company-wide information audit to identify and assess what personal information we hold, where it comes from, how and why it is processed and if and to whom it is disclosed.
- ***Policies & Procedures*** **- [revising/implementing new]** data protection policies and procedures to meet the requirements and standards of the GDPR and any relevant data protection laws, including: -

- ***Data Protection*** – our main policy and procedure document for data protection has been overhauled to meet the standards and requirements of the GDPR. Accountability and governance measures are in place to ensure that we understand and adequately disseminate and evidence our obligations and responsibilities; with a dedicated focus on privacy by design and the rights of individuals.
- ***Data Retention & Erasure*** – we have updated our retention policy and schedule to ensure that we meet the *'data minimisation'* and *'storage limitation'* principles and that personal information is stored, archived and destroyed compliantly and ethically. We have dedicated erasure procedures in place to meet the new *'Right to Erasure'* obligation and are aware of when this and other data subject's rights apply; along with any exemptions, response timeframes and notification responsibilities.
- ***Data Breaches*** – our breach procedures ensure that we have safeguards and measures in place to identify, assess, investigate and report any personal data breach at the earliest possible time. Our procedures are robust and have been disseminated to all employees, making them aware of the reporting lines and steps to follow.
- ***International Data Transfers & Third-Party Disclosures*** – where **Casadh CLG** stores or transfers personal information outside the EU, we have robust procedures and safeguarding measures in place to secure, encrypt and maintain the integrity of the data. Our procedures include a continual review of the countries with sufficient adequacy decisions, as well as provisions for binding corporate rules; standard data protection clauses or approved codes of conduct for those countries without. We carry out strict due diligence checks with all recipients of personal data to assess and verify that they have appropriate safeguards in place to protect the information, ensure enforceable data subject rights and have effective legal remedies for data subjects where applicable.
- ***Subject Access Request (SAR)*** – we have revised our SAR procedures to accommodate the revised 30-day timeframe for providing the requested information and for making this provision free of charge. Our new procedures detail how to verify the data subject, what steps to take for processing an access request, what exemptions apply and a suite of response templates to ensure that communications with data subjects are compliant, consistent and adequate.
- ***Legal Basis for Processing*** - we are reviewing all processing activities to identify the legal basis for processing and ensuring that each basis is appropriate for the activity it relates to. Where applicable, we also maintain records of our processing activities, ensuring that our obligations under Article 30 of the GDPR and Schedule 1 of the Data Protection Bill are met.
- ***Privacy Notice/Policy*** – we are revising our Privacy Notice(s) to comply with the GDPR, ensuring that all individuals whose personal information we process have been informed of why we need it, how it is used, what their rights are, who the information is disclosed to and what safeguarding measures are in place to protect their information.
- ***Obtaining Consent*** – we are revising our consent mechanisms for obtaining personal data, ensuring that individuals understand what they are providing, why and how we use it and giving clear, defined ways to consent to us processing their information. We have developed stringent processes for recording consent, making sure that we can evidence an affirmative opt-in, along with time and date records; and an easy to see and access way to withdraw consent at any time.
- ***Direct Marketing*** – we are revising the wording and processes for direct marketing, including clear opt-in mechanisms for marketing subscriptions; a clear notice and method for opting out and providing unsubscribe features on all subsequent marketing materials.
- ***Data Protection Impact Assessments (DPIA)*** – where we process personal information that is considered high risk, involves large scale processing or includes special category/criminal conviction data; we have developed stringent procedures and assessment templates for carrying out impact assessments that comply fully with the GDPR's Article 35 requirements. We have implemented documentation processes

that record each assessment, allow us to rate the risk posed by the processing activity and implement mitigating measures to reduce the risk posed to the data subject(s).

- ***Processor Agreements*** – where we use any third-party to process personal information on our behalf (*i.e. Payroll, Recruitment, Hosting etc*), we have drafted compliant Processor Agreements and due diligence procedures for ensuring that they (*as well as we*), meet and understand their/our GDPR obligations. These measures include initial and ongoing reviews of the service provided, the necessity of the processing activity, the technical and organisational measures in place and compliance with the GDPR.
- ***Special Categories Data* -** where we obtain and process any special category information, we do so in complete compliance with the Article 9 requirements and have high-level encryptions and protections on all such data. Special category data is only processed where necessary and is only processed where we have first identified the appropriate Article 9(2) basis or the Data Protection Bill Schedule 1 condition. Where we rely on consent for processing, this is explicit and is verified by a signature, with the right to modify or remove consent being clearly signposted.

Data Subject Rights

In addition to the policies and procedures mentioned above that ensure individuals can enforce their data protection rights, we provide easy to access information via **[our website, in the office, during induction etc]** of an individual's right to access any personal information that **Casadh CLG** processes about them and to request information about: -

- What personal data we hold about them
- The purposes of the processing
- The categories of personal data concerned
- The recipients to whom the personal data has/will be disclosed
- How long we intend to store your personal data for
- If we did not collect the data directly from them, information about the source
- The right to have incomplete or inaccurate data about them corrected or completed and the process for requesting this
- The right to request erasure of personal data (*where applicable*) or to restrict processing in accordance with data protection laws, as well as to object to any direct marketing from us and to be informed about any automated decision-making that we use
- The right to lodge a complaint or seek judicial remedy and who to contact in such instances

Information Security & Technical and Organisational Measures

Casadh CLG takes the privacy and security of individuals and their personal information very seriously and take every reasonable measure and precaution to protect and secure the personal data that we process. We have robust information security policies and procedures in place to protect personal information from unauthorised access, alteration, disclosure or destruction and have several layers of security measures, including: -

[insert measures such as SSL, access controls, password policy, encryptions, pseudonymisation, practices, restriction, IT, authentication etc]

GDPR Roles and Employees

Casadh CLG have designated **[insert DPO/lead name]** as our **[Data Protection Officer (DPO)/Appointed Person]** and have appointed a data privacy team to develop and implement our roadmap for complying with the new data protection Regulation. The team are responsible for promoting awareness of the GDPR across the organisation, assessing our GDPR readiness, identifying any gap areas and implementing the new policies, procedures and measures.

Casadh CLG understands that continuous employee awareness and understanding is vital to the continued compliance of the GDPR and have involved our employees in our preparation plans. We have implemented an employee training program specific to the which will be provided to all employees prior to May 25th, 2018, and forms part of our induction and annual training program.

If you have any questions about our preparation for the GDPR, please contact **[Data Protection Officer (DPO)/Appointed Person].**

The Data Protection Principles

The following key principles are enshrined in the Irish legislation and are fundamental to the Casadh CLG 's Data Protection policy.

In its capacity as Data Controller, Casadh CLG ensures that all data shall:

1. ... be obtained and processed fairly and lawfully.

For data to be obtained fairly, the data subject will, at the time the data are being collected, be made aware of:

- The identity of the Data Controller (Casadh CLG)
- The purpose(s) for which the data is being collected
- The person(s) to whom the data may be disclosed by the Data Controller
- Any other information that is necessary so that the processing may be fair.

Casadh CLG will meet this obligation in the following way.

- Where possible, the informed consent of the Data Subject will be sought before their data is processed;
- Where it is not possible to seek consent, Casadh CLG will ensure that collection of the data is justified under one of the other lawful processing conditions – legal obligation, contractual necessity, etc.;
- Where Casadh CLG intends to record activity on CCTV or video, a Fair Processing Notice will be posted in full view;
- Processing of the personal data will be carried out only as part of Casadh CLG 's lawful activities, and Casadh CLG will safeguard the rights and freedoms of the Data Subject;
- The Data Subject's data will not be disclosed to a third party other than to a party contracted to Casadh CLG and operating on its behalf.

2. .... be obtained only for one or more specified, legitimate purposes.

Casadh CLG will obtain data for purposes which are specific, lawful and clearly stated. A Data Subject will have the right to question the purpose(s) for which Casadh CLG holds their data, and Casadh CLG will be able to clearly state that purpose or purposes.

3. ..... not be further processed in a manner incompatible with the specified purpose(s).

Any use of the data by Casadh CLG will be compatible with the purposes for which the data was acquired.

4. .... be kept safe and secure.

Casadh CLG will employ high standards of security in order to protect the personal data under its care. Appropriate security measures will be taken to protect against unauthorised access to, or alteration, destruction or disclosure of any personal data held by Casadh CLG in its capacity as Data Controller.

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

5. ... be kept accurate, complete and up-to-date where necessary.

Casadh CLG will:

- ensure that administrative and IT validation processes are in place to conduct regular assessments of data accuracy;

- conduct periodic reviews and audits to ensure that relevant data is kept accurate and up-to-date. Casadh CLG conducts a review of sample data every six months to ensure accuracy; Staff contact details and details on next-of-kin are reviewed and updated every two years.
- conduct regular assessments in order to establish the need to keep certain Personal Data.

6. ***... be adequate, relevant and not excessive in relation to the purpose(s) for which the data were collected and processed.***

Casadh CLG will ensure that the data it processes in relation to Data Subjects are relevant to the purposes for which those data are collected. Data which are not relevant to such processing will not be acquired or maintained.

7. ***... not be kept for longer than is necessary to satisfy the specified purpose(s).***

Casadh CLG has identified an extensive matrix of data categories, with reference to the appropriate data retention period for each category. The matrix applies to data in both a manual and automated format.

Once the respective retention period has elapsed, Casadh CLG undertakes to destroy, erase or otherwise put this data beyond use.

8. ***... be managed and stored in such a manner that, in the event a Data Subject submits a valid Subject Access Request seeking a copy of their Personal Data, this data can be readily retrieved and provided to them.***

Casadh CLG has implemented a Subject Access Request procedure by which to manage such requests in an efficient and timely manner, within the timelines stipulated in the legislation.

Data Subject Access Requests

As part of the day-to-day operation of the organisation, Casadh CLG 's staff engage in active and regular exchanges of information with Data Subjects. Where a formal request is submitted by a Data Subject in relation to the data held by Casadh CLG , such a request gives rise to access rights in favour of the Data Subject.

There are specific time-lines within which Casadh CLG must respond to the Data Subject, depending on the nature and extent of the request. These are outlined in the attached Subject Access Request process document.

Casadh CLG 's staff will ensure that, where necessary, such requests are forwarded to the Data Protection Officer in a timely manner, and they are processed as quickly and efficiently as possible, but within not more than 40 days from receipt of the request.

Implementation

As a Data Controller, Casadh CLG ensures that any entity which processes Personal Data on its behalf (a Data Processor) does so in a manner compliant with the Data Protection legislation.

Failure of a Data Processor to manage Casadh CLG 's data in a compliant manner will be viewed as a breach of contract, and will be pursued through the courts.

Failure of Casadh CLG 's staff to process Personal Data in compliance with this policy may result in disciplinary proceedings.

Definitions

For the avoidance of doubt, and for consistency in terminology, the following definitions will apply within this Policy.

Data	This includes both automated and manual data. Automated data means data held on computer, or stored with the intention that it is processed on computer. Manual data means data that is processed as part of a relevant filing system, or which is stored with the intention that it forms part of a relevant filing system.
Personal Data	Information which relates to a living individual, who can be identified either directly from that data, or indirectly in conjunction with other data which is likely to come into the legitimate possession of the Data Controller. (If in doubt, Casadh CLG refers to the definition issued by the Article 29 Working Party, and updated from time to time.)
Sensitive Personal Data	A particular category of Personal data, relating to: Racial or Ethnic Origin, Political Opinions, Religious, Ideological or Philosophical beliefs, Trade Union membership, Information relating to mental or physical health, information in relation to one's Sexual Orientation, information in relation to commission of a crime and information relating to conviction for a criminal offence.
Data Controller	A person or entity who, either alone or with others, controls the content and use of Personal Data by determining the purposes and means by which that Personal Data is processed.
Data Subject	A living individual who is the subject of the Personal Data, i.e. to whom the data relates either directly or indirectly.
Data Processor	A person or entity who processes Personal Data on behalf of a Data Controller on the basis of a formal, written contract, but who is not an employee of the Data Controller, processing such Data in the course of his/her employment.
Data Protection Officer	A person appointed by Casadh CLG to monitor compliance with the appropriate Data Protection legislation, to deal with Subject Access Requests, and to respond to Data Protection queries from staff members and service recipients
Relevant Filing System	Any set of information in relation to living individuals which is not processed by means of equipment operating automatically (computers), and that is structured, either by reference to individuals, or by reference to criteria relating to individuals, in such a manner that specific information relating to an individual is readily retrievable.