# The Crystal Therapy Council Data Protection Policy

## Introduction

The purpose of this document is to provide a concise policy statement regarding the Data Protection obligations of the Crystal Therapy Council. 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 Data Protection Act (1988), and the European Union General Data Protection Regulation (GDPR) (2018).

## Rationale

The Crystal Therapy Council must comply with the Data Protection principles set out in the relevant legislation and regulation. This Policy applies to all Personal Data collected, processed and stored by The Crystal Therapy Council in relation to its service providers and clients in the course of its activities.

## Scope

The policy covers both personal and sensitive personal data held in relation to data subjects by The Crystal Therapy Council. The policy applies equally to personal data held in manual and automated form.

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

## Mandala Complementary Studies works as a Data Controller for The Crystal Therapy Council

In the course of its daily organisational activities, the Data Processing Officer (Sue Lilly) acquires, processes and stores data in relation to:

- registered schools of The Crystal Therapy Council

Due to the nature of the service provided by The Crystal Therapy Council there is regular exchange of data between The Crystal Therapy Council and its registered schools. This policy provides the guidelines for this exchange of information.

## The Data Protection Principles

The following key principles are enshrined in the Irish legislation and EU Regulation and are fundamental to The Crystal Therapy Council's Data Protection policy.

In its capacity as Data Controller, Mandala Complementary Studies (registered with the ICO) 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 - Mandala Complementary Studies
- 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.

The Data Controller 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, The Data Controller will ensure that collection of the data is justified under one of the other lawful processing conditions – legal obligation, contractual necessity, etc.;
- Processing of the personal data will be carried out only as part of The Crystal therapy Council's lawful activities, and Mandala Complementary Studies will safeguard the rights and freedoms of the Data Subject;
- The Data Subject's data will not be disclosed to a third party.

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

The Data Controller 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 The Data Controller holds their data, and The Data Controller 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 The Data Controller will be compatible with the purposes for which the data was acquired.

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

The Data Controller 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 the Data Controller. Access to and management of customer records is limited to those who have appropriate authorisation and password access.

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

The Data Controller will:

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

The Data Controller 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).*

The Data Controller keeps personal data for a time deemed reasonable and necessary. Once the period has elapsed, The Data Controller 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.*

The Data Controller 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 Requests

### Subject Access Requests

Any formal, written request by a Data Subject for a copy of their personal data will be processed as soon as possible, with the maximum response time being one month as per GDPR.

### Rectification Requests

Any formal, written request by a Data Subject for the update of their personal data to rectify incorrect or out-of-date information will be carried out within one month.

### Erasure Requests

Any formal, written request by a Data Subject for the erasure or 'right to be forgotten' of their personal data will be carried out within one month.

# Data Breach Reporting

A breach is a loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users, for an authorized purpose, have access or potential access to personal data in usable form, whether manual or automated.

All incidents (a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed) will be reported to the Office of the Data Protection Commissioner within 72 hours. Where devices or equipment containing personal or sensitive personal data are lost or stolen, the Data Protection Commissioner is notified only where the data on such devices is not encrypted. The affected data subjects will also be informed.

# Data Breach Logging

All data breaches will be recorded in an incident log as required by the Office of the Data Protection Commissioner. The log will maintain a summary record of each incident which has given rise to a risk of unauthorised disclosure, loss, destruction or alteration of personal data. The record will include a brief description of the nature of the incident and an explanation of why the Office of the Data Protection Commissioner was not informed. Such records will be provided to the Office of the Data Protection Commissioner upon request.

# 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.<br>Automated data means data held on computer, or stored with the intention that it is processed on computer.<br>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, [The Company] 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. |
| **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. |