IACST
Irish Association of Craniosacral Therapists

Data Protection Policy

Issue Number	1	
Number of Pages	15	
Prepared By	IACST	
Implementation By	IACST Craniosacral Therapists members IACST, Administration Personnel	
Next Review Due	August 2024	
Agreed and Signed By	IACST Committee	Date: August 2021

Contents

1.0 Policy Introduction

1.1 Legislation

The General Data Protection Regulation (GDPR) is an EU Regulation, which is in effect since 25th May 2018. The GDPR, (together with the Data Protection Act 2018); places greater accountability and transparency obligations on all practitioners when using personal information; and gives the individual greater control over their personal information. This includes a right to object to the processing of personal information where that processing is carried out for the delivery of services.

Many therapists are worried about GDPR and what it means to their business or practice. It is important to note that there is no specific regulation for CST therapists or any other independent therapist working in the health sector. This document sets out agreed and reasonable guidance given the nature of and type of business that craniosacral therapy entails.

This guidance is framed within the most current data protection regulations. It does not constitute formal legal advice or official government guidance but guides best practice for practitioners who as Data Controllers are required to be mindful and committed of an individual's right to privacy in all aspects of processing personal and /or sensitive data.

1.2 Policy Purpose and Scope

This policy is a guidance document:

To assist the IACST and its members to meet its legal obligations under the data protection regulations and to ensure that all personal and special category information is processed compliantly and, in the individuals, best interest.

Applies to the IACST , its members and to any individual who conducts work on behalf of the IACST e.g. administrative personnel.

1.3 Definitions

- **Personal data**

Data (manual, automated and verbal) which relates to a living individual who is or can be identified, either from that data itself or from the data in conjunction with other information. Personal data can be held or transmitted in paper, hard copy physical files, electronic files, or communicated verbally in conversation or over the telephone. Appendix A gives examples of Personal Data

- **Data Subject**

A living person who is either identified or identifiable (such a person is referred to as a 'data subject').The individual who is the subject of personal data.

Data Controller

"A ‘controller’ refers to a person, company, or other body that decides how and why a data subject’s personal data are processed. If two or more persons or entities decide how and why personal data are processed, they may be ‘joint controllers’, and they would both share responsibility for the data processing obligations." *https://www.dataprotection.ie/*

Controllers have a range of obligations under data protection law, and in particular must comply with the principles of data protection, as found in Article 5 GDPR, ensuring personal data are: processed lawfully, fairly and transparently; processed for specific purposes; limited to what is necessary; kept accurate and up to date; stored for no longer than necessary; and protected against unauthorised or unlawful processing, accidental loss, destruction, or damage. Controllers must also be able to demonstrate compliance with these principles, under the principle of accountability.

Data Processor

The processor or data processor is a person or organization who deals with personal data as instructed by a controller for specific purposes and services offered to the controller that involve personal data processing (remembering that processing can be really many things under the GDPR)

Data Processing

The performance of any operation on data which may include:

- Collecting, recording, keeping, or using the data
- Organising, storing, structuring, altering the data
- Retrieving or consulting the data
- Disclosing, combining or destroying the data

Sensitive/Special Category Data

data relating to racial/ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sexual life/orientation, genetic or biometric data for the purpose of uniquely identifying a natural person (to include physical characteristics such as signatures or images), or medical information. Note: Personal data relating to criminal convictions and offences is considered in the same manner as sensitive/special category. Financial information does not form part of this category.

Subject Access Request

The right of access, commonly referred to as subject access, gives individuals the right to obtain a copy of *their personal data*, as well as other supplementary information. It helps individuals to understand how and why you are using their data, and check you are doing it lawfully.

Data Portability

Allows data subjects to obtain data that a data controller holds on them and to reuse it for their own purposes.

PDSS (Personal Data Security Schedule)

The primary document used, at a unit or research project level, to record the categories of personal data being processed.

Data Protection Impact Assessment(DPIA)

A way to systematically and comprehensively analyse the personal data processing you engage in or plan to engage in and help you identify and minimise data protection risks.

The Data Protection Commission

The Data Protection Commission (DPC) is responsible for upholding the fundamental right of individuals in the European Union to have their personal data protected. It monitors organisations to make sure that they comply with the GDPR and other data protection legislation. It can also deal with complaints in relation to data protection breaches.

2.0 Data Protection Principles

As Data Controllers, The IACST and its members will endeavour to meet its legal responsibilities in relation to the information it processes. The involves an obligation on all members and therapists involved in processing personal data to apply the 7 fundamental Data Protection Principles / Rules referenced below.

2.1 Obtain and process information fairly

Personal data can be obtained directly from the Data Subject concerned or from third parties e.g. HSE, family members, medical professionals, references, Garda Vetting etc. At the time their personal data is being collected, Data Subjects must be made aware of who is collecting the information, why, who it will be shared with, how long it will be retained and their rights under GDPR.

To process personal data, you must have at least one of the following legal reasons

- The Data Subject has given their consent to that/those specific purpose(s).
- Processing is necessary for the performance of a contract to which the Data Subject is party to / take steps requested by the Data Subject prior to entering a contract.
- Processing is necessary for compliance with a Controller's legal obligation.
- Processing is necessary to protect the vital interests of the Data Subject or another natural person.
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official duty vested in the controller.
- Processing is necessary for the purposes of the legitimate interests perused by the Controller or third party (Processor), except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject which require protection of personal data, in particular where the Data Subject is a child.

Sensitive/Special Category Data requires an additional level of protection. Processing of these special categories is prohibited, except in limited circumstances set out in Article 9 of the GDPR.

To process sensitive/special category data you must satisfy one of the following additional conditions:

- The Data Subject has given their explicit consent to that/those specific purpose(s).

- Processing is necessary to carry out the obligations of the Controller/Data Subject in the field of employment or social security and social protection.
- Processing is necessary to protect the vital interests of the Data Subject or of another person where the Data Subject is incapable of giving consent.
- Processing is carried out for legitimate activities with appropriate safeguards by a foundation, association or any other non-profit-seeking body with a philosophical or religious aim in connection with its ethos and purposes.
- Processing relates to personal data which are manifestly made public by the Data Subject.
- Processing is necessary for the establishment, exercise or defence of legal claims.
- Processing is necessary for reasons of substantial public interest.
- Processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services pursuant to a contract with a health professional.
- Processing is necessary for reasons of public interest in the area of public health.
- Processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with the Regulation.

2.2 Consent

Where consent is required to process information, the consent must be freely given from the outset, it must be clear, intelligible, and the individual must be able to withdraw consent in a way that is as free as they have given it. Inferred consent is not enough, it must be explicit (e.g. no pre-ticked boxes).

2.3 Process Personal Data only for one or more specified, explicit and lawful purpose

- Only process Personal Data for purposes that are specific, lawful and clearly stated.
- Personal Data must be used in a way that meets those purposes that people have consented to or could reasonably expect

2.4 Process Personal Data in ways compatible with the purposes for which it was initially given. Keep it adequate, relevant and not excessive

All processing of data must be limited to the minimum necessary to achieve the purpose(s).. If you don't need the information, don't ask for it!

2.5 Keep Personal Data accurate and up-to-date

Amendments must be actioned as quickly as possible, particularly where data has been identified and agreed as incorrect.

Therapists are responsible for informing the IACST of any changes to their personal details e.g. change of address.

2.6 Retain Personal Data only for as long as is necessary for the specified purpose(s)

CST Therapist should be clear about the length of time for which Personal Data will be kept and why.

Client records must be kept after the person has stopped being a client – unless the client asks you to destroy them.

There are no clear rules on how long you should keep them. The Data Protection Agency is currently saying seven years as all other business records have to be kept for seven years.

Records for children and young people should be retained until the client is 25 (or 26 if they are 17 when therapy sessions end) or 8 years after their death, if sooner.

2.7 Keep Personal Data safe and secure

The IACST promotes high standards of security for all Personal Data. At all times when data is in the practitioners care, you must keep it safe and secure from unlawful or unauthorised access, modification or deletion. This applies to the point where the data is actually destroyed/archived.

Physical Security

- Paper records are be maintained in locked filing cabinets, particularly when you are away from your desk for long periods and at the end of each day.
- Office doors are be locked when unoccupied.
- Information on computer screens and paper files are to be kept out of sight from callers to a practice setting.
- Double check when addressing emails to the correct person, and you are not cc'ing anyone who does not need/should not have the information.

IT Security

- Ensure the device locks automatically either via password, pin, fingerprint or other security system.
- Passwords/PINS/Encryption are to be enacted on all electronic and portable devices, (e.g. Mobile phones, USB keys).
- Limit the personal data held on portable devices where possible (i.e. mobile phones, USB keys).
- Access to data on relevant systems within the IACST is restricted to authorised staff for business purposes, and is password protected/encrypted where possible.
- Formally log out of email, don't just close the browser or phone – that leaves the connection open.
- Lock your PC or laptop when leaving it unattended.
- Formally log out of email, don't just close the browser or phone – that leaves the connection open.
- Only download client data into the device if you absolutely have to in order to deliver the service, and delete it as soon as possible afterwards.

General

- Where possible, try not to discuss personal or sensitive information about an individual in a place where the discussion can be openly heard.
- Only take physical files from their usual location when necessary. When transporting the file, do what is necessary to keep it safe and ensure it is under your control.
- Shred unwanted hard copy personal information, do not throw it in the bin

2.7 Be Compliant

The legislation requires that we are “responsible for, and be able to demonstrate compliance with the GDPR principles” referred to in Section 2 of this document. This means that we must:

- Adhere to the 7 principles outlined.
- Keep relevant documentation and logs on data processing activities.
- Consider privacy by 'design and default' at every step of processing.
- Implement measures that aim to ensure and demonstrate your compliance with the legislation.
- Record all Data Breaches.

3.0 Data Breach Management

3.1 What is a Data Breach?

A personal data breach means a breach of security leading to the accidental or unlawful. destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. The term 'personal data' means any information concerning or relating to an identified or. identifiable individual. Examples of Data Breaches may include the following:
(a) Loss, theft or misplacement of IT equipment or devices containing personal data e.g. laptop, Smartphone or USB key.
(b) Loss, theft or misplacement of a folder, briefcase or diary containing personal data;
(c) Human error resulting in an email or piece of post containing personal data being sent to the wrong person.
(d) An attack by a “hacker” which results in unauthorised access to our computer systems;
(e) Unauthorised access to personal data as a result of aa# break-in.
(f) Unauthorised access to personal data by deception.
(g) Unauthorised access to personal data as a result of breaching access rights.
(h) Unforeseen circumstances such as flood or fire where personal data is inaccessible.
(i) Where personal data has been deleted in error and the data cannot be restored.

3.2 When should I report a suspected Data Breach? To whom?

Immediately.

The controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Data Protection Commissioner, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay. The notification shall describe in clear and plain language the nature of the personal data breach and contain at least:

- The name and contact details of the data protection officer or other contact point where more information can be obtained;

- A description of the likely consequences of the personal data breach;
- A description of the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects

A notification of a personal data breach by a controller to the DPC can be done through the breach notification form on the DPC's website. https://www.dataprotection.ie/

Appendix C contains a copy of the Data Breach Form. Whilst the form is not mandatory, any report of a breach should at least contain the information requested within this form.

4.0. Data Subject Rights

The legislation gives the following rights to individuals:

(a) The right to be informed.

(b) The right to rectification.

(c) The right to erasure.

(d) The right to restrict processing.

(e) The right to portability of data.

(f) The right to object.

(g) Rights in relation to automated decision making and profiling

(h) The right of access. Under Article 15 of the GDPR, an individual has the right to obtain from any agency or practitioner confirmation as to whether personal data concerning them is being processed. Requests must be made in writing to the therapist or an Organisation's Data Protection Officer, and a response should issue within 30 days. Subject Access Template Access request form can be found in Appendix D.

Children's personal data

Children have the same data protection rights as adults and can make access requests. However, they are given specific protection with regard to their personal data. This is because they may be less aware of the risks and consequences of sharing their personal data. Also, they may be less aware of the safeguards available and their rights in relation to how their personal information is processed.

Parents and guardians may also be able to make access requests or exercise any other data protection right on behalf of their children. If a request is made by a parent or guardian, the data controller must consider the nature and circumstances of the request, including the age, capacity and views of the child and the child's best interests.

5.0 Training and Supports

All members of the IACST (to include students and administrative personnel) must consider Data Protection issues as key in their role. The following are useful links to resources about Data Protection.

- The Data Protection Commission has prepared a series of PowerPoint presentations on different aspects of data protection which are available on its website and on You tube. (www.youtube.com/dataprotection).
- There is further detailed information about the GDPR on dataprotection.ie.
- https://www.dataprotection.ie/sites/default/files/uploads/2019-10/Data%20Breach%20Notification_Practical%20Guidance_Oct19.pdf
- The Citizens Information Board offers a number of key and related accessible documents on GDPR which can be accessed on its website.
- https://www.citizensinformation.ie/en/government_in_ireland/data_protection/overview_of_general_data_protection_regulation.html#
- Free GDPR Resources
- https://www.itgovernance.eu/en-ie/gdpr-resources-ie
- A number of short online courses are available on General Data Protection Regulation training e.g. HSE

The IACST recommends that members should take the time to complete one of the online courses on offer.

6.0 Research

Enacted in 2018, and amended in 2021 , the Irish Health Research Regulations provide for "suitable and specific measures" for the processing of personal data for the purpose of health research, to protect the rights and freedoms of research participants.

References

https://www.hse.ie/eng/gdpr/gdpr-faq/hse-gdpr-faqs-public.pdf

(GDPR)https://www.citizensinformation.ie/en/government_in_ireland/data_protection/overview_of_general_data_protection_regulation.html

https://www.dataprotection.ie/sites/default/files/uploads/2019-04/The-GDPR-and-You-2.pdf

https://www.dataprotection.ie/sites/default/files/uploads/2019-04/A-Guide-to-help-SMEs-Prepare-for-the-GDPR.pdf

https://www.dataprotection.ie/en/organisations/know-your-obligations/data-protection-officers

https://www.google.com/search?rlz=1C1GGRV_enIE763IE775&lei=4cQnYfjVNPG58gKBurvwBA&q=data%20protection%20act

https://www.hrb.ie/funding/gdpr-guidance-for-researchers/

https://www.eui.eu/documents/servicesadmin/deanofstudies/researchethics/guide-data-protection-research.pdf

http://www.irishstatutebook.ie/eli/2021/si/18/made/en/print

Appendix A

Examples of personal data/special category personal data may include:

 Name, address, date of birth, telephone number

 Bank account details

 Expense Claims

 Online identifiers (such as an IP address)

 Location data

 Salary details

 Garda Vetting

 Medical Records/Doctor's notes or certificates

 Annual leave records

 CCTV images / Voice Recordings / Video Footage

 Signatures

 Professional development / Training records

 Photographs

 Consent Forms

 Mailing lists / checklists of attendees

 Examination records

 Correspondence with any individual

 Feedback forms

 Application forms

 Clinical files

 Bank details of suppliers who are individuals

(i.e. not legal entities such as companies/trusts)

 Curriculum Vitae

 Payslip

 Disciplinary issues

 Car Registration Details

This list aims to provide some examples but is not exhaustive, there are many more.

Appendix B

(i) Example of Consent Form for the Use of Photographs / Videos

In order to be compliant with the General Data Protection Regulation (GDPR), ----------permission to use images of you, as an image is classed as sensitive personal data or special category data. We would like to get this permission to possibly use your image for the following purposes: ***(Please tick the box beside each option to indicate your consent)*** • Publication on the …….website / …….. employed electronic systems • Annual Reports / Marketing Materials • Teaching / Documentary Materials …… will not use the images / recordings for any purpose other than those consented to above. You have the right to ask us to stop using your image at any time. However it is important to recognise that once published, requests for destruction of that image may not be fully possible. This is particularly important where images are used for published material, and material which ……. is legally obliged to retain, for example Annual Reports.
1. Consent:
I have read and understand the conditions and consent to my image being used as determined above. **Signature: _____ Date: _____**
2. Consent via Authorised Representative / Guardian *(Only complete this section if you are acting as the authorised representative/guardian of a client . Additional information is requested in this section, in order to be assured of your identity)*
Clients Name:
My relationship to Client **User:**
My telephone No:
My Address:
My E-mail Address
I confirm that I am the *authorised* representative/guardian of the client referred within, I have read and **understand the conditions and consent to his/her image being used as determined above:**
Representative's Signature: _____ Date: _____
3. Contact Details
*If you have any questions in relation to this consent form, or the way in which your information/image may be used please contact**:***

Appendix C

Data Breach Form Template

This template may be used as a recording tool in conjunction with the Protocol for Managing a Data Breach

Incident Details

Description of the incident	
Date and time incident occurred	
Name of individual reporting the incident	
Incident reported to DPC	
Type of data involved. Any data of a sensitive nature	
No. of individuals affected by the breach	
Cause of the incident	
Were affected individuals contacted?	
Was the data encrypted or anonymised?	
Details of any IT systems involved in the breach	

Appendix D

Subject Access Request Template

Dear...

I wish to make an access request under Article 15 of the General Data Protection Regulation (GDPR) for a copy of any information you keep about me, on computer or in manual form in relation to...

https://www.dataprotection.ie/en/individuals/know-your-rights/right-access-information