SENIOR CITIZENS CONCERN CLG
DATA PROTECTION POLICY & PROCEDURES

Contents

1 BACKGROUND

Senior Citizens Concern CLG was set up to provide Day care and housing services for older citizens in our Community at our Day Care Centre and other venues. Based in the South West of Co. Wexford, covering the parishes of Ramsgrange, Duncannon, Horeswood, Templetown and Tintern. We provide Day Care, Transport, Nursing & Medical Care to those who attend the centre, also Physiotherapy, Chiropody, Hairdressing, Laundry service, an advice service, sheltered housing, meals-on-wheels, fresh baking, educational and recreational activities. Limited Voluntary Housing Service Available. The Centre in Ramsgrange is open to clients daily from Monday to Friday and Meals on Wheels are also provided Monday to Friday. Active Retirement meet the first Monday of every month and have regular soical evenings each month.

2 OUR MISSION

To provide care, opportunity for social interaction and other essential services to promote independence for older people in our community.

3 POLICY STATEMENT

The collection and storing of personal information, including sensitive (special category) personal information is fundamental to our service, in order to provide our service users with the highest standard of care and support. Personal data is collected from employees, clients, suppliers, partners, regulators and other third parties and includes *inter alia,* name, address, email address, data of birth, identification numbers, private and confidential information, sensitive medical information and bank/credit card details.

In addition, we may collect and use certain types of personal information to comply with certain laws and/or regulations. However, we are committed to processing all personal information in accordance with the ***General Data Protection Regulation (GDPR)***, ***Irish data protection laws*** and any other relevant the data protection laws and codes of conduct ***("data protection laws").***

These and the associated policies, procedures, controls and measures, ensure compliance with data protection laws.

4 PURPOSE

The purpose of this policy is to ensure that we meet our legal, statutory and regulatory requirements under data protection laws and to ensure that all personal, sensitive and special category information "Data" is processed fairly and in compliance with the law as well as in an individual's best interest.

We have put comprehensive measures in place to promote accountability and governance. The aim of such measures is to ultimately minimise the risk of breaches and uphold the protection of personal data and its integrity. This policy also serves as a reference document for employees and third-parties on the responsibilities of handling and accessing personal data and Data Subject requests.

5 SCOPE

This policy applies to all staff. Adherence to this policy is mandatory and non-compliance could lead to disciplinary action.

5.1 DEFINITIONS

- ***"Consent"*** of the Data Subject means any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
- ***"Data controller"*** means, the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.
- ***"Data processor"*** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
- ***"Data Subject"*** means an individual who is the subject of personal data
- ***"GDPR"*** means the *General Data Protection Regulation (EU) (2016/679)*
- ***"Genetic data"*** means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.
- ***"Personal Data"*** means any information relating to an identified or identifiable natural person *('Data Subject'*); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- ***"Processing"*** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- ***"Recipient"*** means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.
- ***"Supervisory Authority"*** means the ODC.
- ***"Third Party"*** means a natural or legal person, public authority, agency or body other than the Data Subject, under our direct authority.

6 DATA PROTECTION BACKGROUND

6.1 GENERAL DATA PROTECTION REGULATION (GDPR)

The ***General Data Protection Regulation (GDPR) (EU)2016/679)*** was approved by the European Commission in April 2016 and will apply to all EU Member States from 25th May 2018. As a *'Regulation*' rather than a *'Directive'*, its rules apply directly to Member States, replacing their existing

local data protection laws and repealing and replacing Directive 95/46EC and its Member State implementing legislation.

As we process personal information regarding individuals (*Data Subjects*), we are obligated under the General Data Protection Regulation (GDPR) to protect such information, and to obtain, use, process, store and destroy it, only in compliance with the GDPR's rules and principles.

6.1.1 PERSONAL DATA

As an organisation which provides a level of care to older people we often need to know and come into possession of very sensitive personal information, in particular medical and health information. We must be particularly careful to ensure that a high level of care is afforded to Personal Data falling within the GDPR's **'special categories'** *(previously **sensitive personal data***) due to the assumption that this type of information could be used in a negative or discriminatory way and is of a sensitive, personal nature to the persons it relates to.

6.1.2 THE GDPR PRINCIPLES

Article 5 of the GDPR requires that personal data shall be: -

a) processed lawfully, fairly and in a transparent manner in relation to the Data Subject ***('lawfulness, fairness and transparency')***

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ***('purpose limitation')***

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ***('data minimisation')***

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay ***('accuracy')***

e) kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the personal data is processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the Data Subject ***('storage limitation')***

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ***('integrity and confidentiality').***

Article 5(2) requires that *'the controller shall be responsible for, and be able to demonstrate, compliance with the data protection laws principles'* ***('accountability')*** and requires that firms ***show***

how they comply with the principles, detailing and summarising the measures and controls that they have in place to protect personal information and mitigate the risks of processing.

6.2 THE OFFICE OF THE DATA PROTECTION COMMISSIONER (ODC)

The ODC is an independent regulatory office whose role it is to uphold data protection and privacy rights in the public interest.

6.3 DATA PROTECTION OFFICER

Articles 37-39, and Recital 97 of the GDPR detail the obligations, requirements and responsibilities on firms to appoint a Data Protection Officer and specifies the duties that the officer themselves must perform.

A Data Protection Officer (DPO) must be appointed where: -

- The data processing is carried out by a public authority or body *(except for courts acting in their judicial capacity);*
- the core activities of the controller/processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of Data Subjects on a large scale
- the core activities of the controller / processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10

It is not deemed to be necessary for us to appoint a DPO however we have appointed our Centre Manager to be the person within our organisation responsible for Data Protection and who shall liaise with the Board of Directors to ensure our compliance with this and the associated policies.

7 OBJECTIVES

We are committed to ensuring that all Personal Data processed by us is done in accordance with data protection laws and its principles. We ensure the safe, secure, ethical and transparent processing of all personal data and have stringent measures to enable Data Subjects to exercise their rights.

We have developed the following objectives to meet our data protection obligations and to ensure continued compliance with legal and regulatory requirements.

We ensure that: -

- We protect the rights of individuals when processing their personal information;
- We develop, implement and maintain a data protection policy, procedure, audit plan and training program for compliance with data protection laws;
- Every function and process carried out by us has been and is on an ongoing basis, assessed for compliance with data protection laws;
- Personal data is only processed where we have satisfied the legal consent and processing requirements;
- We only process special category data in accordance with the GDPR;
- We record consent at the time it is obtained and evidence such consent to the Supervisory Authority where requested to do so;

- All employees are competent and knowledgeable about their GDPR obligations and are provided with training in data protection laws, principles, regulations and how they apply to their specific role and the Company;
- Individuals feel secure when providing us with personal information and know that it will be handled in accordance with their rights under data protection laws;
- We maintain a continuous program of monitoring, review and improvement with regards to compliance with data protection laws and to identify gaps and non-compliance before they become a risk, affecting mitigating actions where necessary;
- We have robust and documented Complaint Handling and Data Breach controls for identifying, investigating, reviewing and reporting any breaches or complaints with regards to data protection;
- We have voluntarily appointed a member of our team (being our Centre Manager) who takes responsibility for the overall supervision, implementation and ongoing compliance with the data protection laws and performs specific duties as set out under Article 37 of the GDPR;
- We store and destroy all personal information, in accordance with our Retention and Erasure Policy which has been developed from the legal, regulatory and statutory requirements and suggested timeframes;
- Any information provided to an individual in relation to personal data held or used about them, will be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language;
- Employees are aware of their own rights under the data protection laws and are provided with the Article 13/14 information disclosures in the form of a Privacy Notice;
- Where applicable, we maintain records of processing activities in accordance with the Article 30 requirements.

8 SECURITY MEASURES

8.1 INTRODUCTION

We take reasonable steps to protect records from loss, misuse or unauthorised access. There are a number of ways in which records can be protected these include:

8.2 PHYSICAL MEASURES

In the case of a manual record system, ensuring that there is no general access from the public areas of the Centre to the offices. File rooms and filing cabinets should be locked when not in use.

Access to computer servers should be restricted and should not be accessible from public areas. Computer servers should be kept in cool, well ventilated rooms and fitted with surge protectors and clearly auxiliary power supply to prevent data loss due to power surge failure.

When disposing of obsolete or redundant equipment we must ensure that all data previously stored on the devices has been removed prior to disposal. It is not sufficient to merely reformat the hard drives of the devices.

8.3 ELECTRONIC MEASURES

Access to the computer's operating system and Company software is password protected.

A IT Security Policy has been put in place. Appropriate Internet security software has been installed. Security updates software patches should be regularly installed.

A robust backup procedure is in place so that if data is corrupted or lost, a recent copy of the electronic records will be available.

See the Information Technology Security Policy document for more information.

8.4 HUMAN MEASURES

All staff will be provided with training. Such training includes *inter alia*:

- how to use the computer and software effectively.
- What to do and who to ask when faced with a problem.
- How to create a good password, change regularly, keep it safe and not share with others in the Company.
- An overview of the importance of service user confidentiality so that service user information is never given out inappropriately, especially over the phone.
- An understanding that neither fax nor email a secure method of transferring service user information. At the faxing is in use as a means of urgent information exchange in general practices, its use should be kept to a minimum.
- Inappropriate use of the internetwork also poses a significant risk to secure of electronic service user records. Staff should be aware of the dangers of accessing certain websites and should only access the internetwork was required for the running of the Company. It is useful to have a clear policy for staff, locums and others outlining what is considered to be appropriate use of the Internet. Please see our Internet use policy and staff Handbook.

8.5 LAPTOPS AND USB STORAGE DEVICES

Laptops and Portable computers are not used. USB storage devices are an extremely risky mode of transferring information. For this reason, no identifiable Client information should be held on USB memory keys. Further guidance is available on the website of the Data Protection Commissioner in relation to security and obligations that arise in the event of a security breach.

Please also see our ***Data Breach Policy***. Also, see our ***Clear Desk Policy*** document for guidance on protecting information on portable electronic devices, both when in-use and not-in use.

8.6 USE OF EMAIL

Documents sent by email are not secure and can be accessed deliberately by others before reaching their intended recipients. For this reason, medical and health information should not be transmitted by email unless it is encrypted or secure electronic pathway has been established.

See ***Email Usage Policy*** document for more information.

8.7 USE OF SMS COMMUNICATION

The use of text or SMS messages to Clients can appear an efficient and attractive way of communicating. There are difficulties however with sending any confidential information in this way as text messages can be read by others and mobile phone numbers can change. It is advisable

therefore to restrict messages by text to non-sensitive matters such as appointment reminders. Client consent is required in order to communicate with Clients by means of text messages.

9 GOVERNANCE PROCEDURES

9.1 ACCOUNTABILITY & COMPLIANCE

Due to the nature, scope, context and purposes of the processing undertaken by us, we carry out frequent risk assessments and information audits to identify, assess, measure and monitor the impact of such processing. We have implemented adequate and appropriate technical and organisational measures to ensure the safeguarding of personal data and compliance with data protection laws and can evidence such measures through our documentation and practices.

9.1.1 PRIVACY BY DESIGN

We operate a *'Privacy by Design'* approach and ethos, with the aim of mitigating the risks associated with processing personal data through prevention via processes, systems and activities. We have developed controls and measures that help us enforce this ethos.

Data Minimisation

Under Article 5 of the GDPR, principle (c) advises that data should be *'limited to what is necessary'*, which forms the basis of our minimalist approach. We only ever obtain, retain, process and share data that is essential for carrying out our services and/or meeting our legal obligations and only retain data for as long as is necessary.

Our systems, employees, processes and activities are designed to limit the collection of personal information to that which is directly relevant and necessary to accomplish the specified purpose. Data minimisation enables us to reduce data protection risks and breaches and supports our compliance with data protection laws.

Restriction

Our *Privacy by Design* approach means that we use Company-wide restriction methods for all personal data activities. Restricting access is built into the foundation of our processes, systems and structure and ensures that only those with authorisation and/or a relevant purpose, have access to personal information. Special category data is restricted at all levels and can only be accessed by those with a clinical requirement to do so or with a legitimate interest in doing so**.**

Hard Copy Data

Due to the nature of our business, it is sometimes essential for us to obtain, process and share personal and special category information which is only available in a paper format without pseudonymisation options (*i.e. copies of service user records, invoices or other information*). Where this is necessary, we utilise a tiered approach to minimise the information we hold and/or the length of time we hold it for.

9.2 LEGAL BASIS FOR PROCESSING *(LAWFULNESS)*

At the core of all personal information processing activities undertaken by us, is the assurance and verification that we are complying with Article 6 of the GDPR and the lawfulness of our processing obligations. Prior to carrying out any personal data processing activity, we identify and establish the legal basis for doing so and verify these against the regulation requirements.

Data is only obtained, processed or stored when we have met the lawfulness of processing requirements, where: -

- The Data Subject has given consent to the processing of their personal data for one or more specific purposes;
- Processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract;
- Processing is necessary for compliance with a legal obligation to which we are subject;
- Processing is necessary in order to protect the vital interests of the Data Subject or of another natural person;
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested us;
- Processing is necessary for the purposes of the legitimate interests pursued by us or by a third party (*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).*

9.2.1 PROCESSING SPECIAL CATEGORY DATA

Special categories of Personal Data are defined in the data protection laws as: -

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited – unless one of the Article 9 clauses applies.

Where we process any personal information classed as special category, we do so in accordance with Article 9 of the GDPR regulations and in compliance with the Data Protection Bill's Schedule 1 Parts 1, 2, 3 & 4 conditions and requirements.

We will only ever process special category data where: -

- The Data Subject has given explicit consent to the processing;
- Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the Data Subject in the field of employment and social security and social protection law;
- Processing is necessary to protect the vital interests of the Data Subject or of another natural person where the Data Subject is physically or legally incapable of giving consent;
- Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim;
- Processing relates to personal data which are manifestly made public by the Data Subject;
- Processing is necessary for the establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity;
- Processing is necessary for reasons of substantial public interest;

- Processing is necessary for the purposes of preventive 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;
- Processing is necessary for reasons of public interest in the area of public health;
- Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1).

Schedule 1, Parts 1, 2 & 3 of The Data Protection Bill provide specific conditions and circumstances when special category personal data can be processed and details the requirements that organisations are obligated to meet when processing such data.

Because we process personal information that falls into one of the above categories, we have adequate and appropriate provisions and measures in place prior to any processing.

9.3 INFORMATION SHOULD BE ACCURATE, COMPLETE AND UP-TO-DATE

Clients may occasionally bring to our attention their concerns about the information held about them. They have the right of correction, rectification, erasure and blocking in relation to information held on them that is not in keeping with the principles of data protection law, for example, inaccurate, non-relevant, excessive information.

As a rule, with every request for alteration correction, the Company should annotate the record to indicate the nature of the request and whether or not they agree with that. For legal reasons, it is inadvisable to attempt to alter or erase the original entries in the medical record, and in some circumstances, it may be unlawful to do so.

Where information has been materially and significantly enhanced, corrected, amended, blocked or deleted, there is a requirement to notify any person to whom it was disclosed within the previous 12 months unless such notification proves impossible or involves disproportionate effort.

It is good practice to ask Clients to review the information held about them on a regular basis, particularly contact information, medical history and allergies to ensure that these are up-to-date and accurate.

High-quality records are:

- organised in a manner that, minimises the potential for one person's information to get confused with another;
- Documented, dated and well-organised for efficient retrieval;
- As detailed as necessary;
- Accurate and current to the greatest extent possible;
- Comprehensive and legible.

9.4 CODES OF CONDUCT & CERTIFICATION MECHANISMS

We have studied and adhere to the data protection advice prepared by Pobal to demonstrate that we comply with data protection laws rules and principles.

9.5 THIRD-PARTY PROCESSORS

We utilise external service providers for certain processing activities.

Such external processing includes** (but is not limited to**): -

- IT Systems and Services;
- CCTV;
- Human Resources and Payroll;
- Hosting or Email Servers;
- Medical/Health services.

Regarding the use of medical and health services we do not exchange and special category information with these service providers. It is our position that in relation to these service providers, we are a processor only on their behalf and they are the Data Controller. We are not party to or privy to the detail of their consultations and only assist in the logistical arrangements required.

We have strict due diligence procedures in place and review, assess and background check all processors prior to forming a business relationship.

The continued protection of Data Subjects' rights and the security of their personal information is always our top priority when choosing a processor and we understand the importance of adequate and reliable outsourcing for processing activities as well as our continued obligations under the data protection laws for data processed and handled by a third-party.

We apply Service Level Agreements (SLAs) and contracts with each processor as per the services provided and have a dedicated Processor Agreement template that details: -

- The processors data protection obligations;
- Our expectations, rights and obligations;
- The processing duration, aims and objectives;
- The Data Subjects' rights and safeguarding measures;
- The nature and purpose of the processing;
- The type of personal data and categories of Data Subjects.

We will ensure that a service provider's SLA either conforms to our own Processor Agreement Template or addresses each of the elements described above to our satisfaction. Each of the areas specified in the contract are monitored, audited and reported on. Processors are notified that they shall not engage another processor without our prior specific authorisation and any intended changes concerning the addition or replacement of existing processors must be done in writing, in advance of any such changes being implemented.

The Processor Agreement and any associated contract reflects the fact that the processor: -

- Processes the personal data only on our documented instructions;
- Seeks our authorisation to transfer personal data to a third country or an international organisation (*unless required to do so by a law to which the processor is subject*);
- Shall inform us of any such legal requirement to transfer data before processing;
- Ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

- Takes all measures to security the personal data at all times;
- Respects, supports and complies with our obligation to respond to requests for exercising the Data Subject's rights;
- Assists us in ensuring compliance with our obligations for data security, mitigating risks, breach notification and privacy impact assessments;
- When requested, deletes or returns all personal data to us after the end of the provision of services relating to processing, and deletes existing copies where possible;
- Makes available to us all information necessary to demonstrate compliance with the obligations set out in the agreement and contract;
- Allows and supports audits, monitoring, inspections and reporting as set out in the contract;
- Informs us immediately of any breaches, non-compliance or inability to carry out their duties as detailed in the contract.

9.6 DATA RETENTION & DISPOSAL

We have defined procedures for adhering to the retention periods set out by the relevant laws, contracts and our business requirements, as well as adhering to the GDPR requirement to only hold and process personal information for as long as is necessary. All personal data is disposed of in a way that protects the rights and privacy of Data Subjects *(e.g. shredding, disposal as confidential waste, secure electronic deletion)* and prioritises the protection of the personal data in all instances.

10 DATA PROTECTION IMPACT ASSESSMENTS (DPIA)

Individuals have an expectation that their privacy and confidentiality will be upheld and respected whilst their data is being stored and processed by us. We therefore utilise several measures and tools to reduce risks and breaches for general processing. However, where processing is likely to be high risk or cause significant impact to a Data Subject, we utilise proportionate methods to map out and assess the impact ahead of time.

Pursuant to Article 35(3) and Recitals 84, 89-96, we consider processing that is likely to result in a high risk to include: -

- Systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person(s);
- Processing on a large scale of special categories of data – Note that processing of personal medical data by an individual general practice isn't considered "processing on a large scale";
- Processing on a large scale of personal data relating to criminal convictions and offences;
- Systematic monitoring of a publicly accessible area on a large scale (i.e. CCTV);
- Where a processing operation is likely to result in a high risk to the rights and freedoms of an individual;
- Those involving the use of new technologies;
- New processing activities not previously used;
- Processing considerable amounts of personal data at regional, national or supranational level,

which could affect many Data Subjects;

- Processing activities making it difficult for the Data Subject(s) to exercise their rights.

Carrying out DPIAs enables us to identify the most effective way to comply with our data protection obligations and ensure the highest level of data privacy when processing. It is part of our Privacy by Design approach and allows us to assess the impact and risk before carrying out the processing, thus identifying and correcting issues at the source, reducing costs, breaches and risks.

The DPIA enables us to identify possible privacy solutions and mitigating actions to address the risks and reduce the impact. Solutions and suggestions are set out in the DPIA and all risks are rated to assess their likelihood and impact. The aim of solutions and mitigating actions for all risks is to ensure that the risk is either: -

- Eliminated
- Reduced
- Accepted

11 DATA SUBJECT RIGHTS PROCEDURES

11.1 CONSENT & THE RIGHT TO BE INFORMED

The collection of personal and sometimes special category data is a fundamental part of the services offered by us and we therefore have specific measures and controls in place to ensure that we comply with the conditions for consent under the data protection laws.

The data protection law defines consent as; *'Any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her'.*

We are required to inform our Service Users of what use will be made of the data we collect and hold including if it will be stored on computer. In general, the service user should be aware of the following;

- what information is being collected?
- why the information is being collected?
- who within us will have access to the information?
- how the information will be used?
- the consequences of not providing the information.
- what third-party disclosures are contemplated, if any?
- that he or she can have access to the information, once collected.

Wherever it is reasonable and practicable to do so, personal health information about the service user should be collected directly from the client rather than from third parties

Where processing is based on consent, we have reviewed and revised all consent mechanisms to ensure that: -

- Consent requests are transparent, using plain language and is void of any illegible terms, jargon or extensive legal terms;

- It is freely given, specific and informed, as well as being an unambiguous indication of the individual's wishes;
- Consent is always given by a statement or a clear affirmative action (*positive opt-in*) which signifies agreement to the processing of personal data;
- Consent mechanisms are upfront, clear, granular (*in fine detail*) and easy to use and understand
- Pre-ticked, opt-in boxes are **never** used;
- Where consent is given as part of other matters (*i.e. terms & conditions, agreements, contracts*), we ensure that the consent is separate from the other matters and is **not** be a precondition of any service (*unless necessary for that service);*
- Along with our Company name, we also provide details of any other third party who will use or rely on the consent;
- Consent is always verifiable, and we have controls in place to ensure that we can demonstrate consent in every case;
- We keep detailed records of consent and can evidence at a minimum: –
    - that the individual has consented to the use and processing of their personal data
    - that the individual has been advised of our Company name and any third party using the data
    - what the individual was told at the time of consent
    - how and when consent was obtained
- We have ensured that withdrawing consent is as easy, clear and straightforward as giving it and is available through multiple options, including: -
    - Opt-out links in mailings or electronic communications
    - Opt-out process explanation and steps on website and in all written communications
    - Ability to opt-out verbally, in writing or by email
- Consent withdrawal requests are processed immediately and without detriment;
- Where services are offered to children, age-verification and parental-consent measures have been developed and are in place to obtain consent;
- For special category data, the consent obtained is explicit *(stated clearly and in detail, leaving no room for confusion or doubt*) with the processing purpose(s) always being specified.

11.1.1 CONSENT CONTROLS

We maintain rigid records of Data Subject consent for processing personal data and are always able to demonstrate that the Data Subject has consented to processing of his or her personal data where applicable. We also ensure that the withdrawal of consent is as clear, simple and transparent and is documented in all instances.

Where the Data Subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent is presented in a manner which is clearly distinguishable from those matters, in an intelligible and easily accessible form, using clear and plain language. All such written declarations are reviewed and authorised by the Centre Manager prior to being circulated.

Consent to obtain and process personal data is obtained by us through: -

- Face-to-Face
- Telephone
- In Writing

Where consent is obtained verbally, we utilise forms to ensure that all requirements have been met and that consent is obtained compliantly and can be evidenced.

Privacy Notices are used in all forms of consent and personal data collection, to ensure that we are compliant in disclosing the information required in the data protection laws in an easy to read and accessible format.

Information should be kept for one or more specific and lawful purpose only.

11.1.2 CHILD'S CONSENT

While the GDPR states that a child's age is defined as 16; the Irish Data Protection Bill proposes to reduce this age to ***13 years***, as per Article 8(1) of the data protection laws what advises that *"Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years."*

The data protection laws state that where processing is based on consent and the personal data relates to a child who is below the age of 13 years such processing is only carried out by us where consent has been obtained by the holder of parental responsibility over the child.

We have mechanisms in place to verify the age of any child prior to obtaining consent and review such consents annually for transferring from parental consent over to the child after age 13.

11.1.3 ALTERNATIVES TO CONSENT

We recognise that there are six lawful bases for processing and that consent is not always the most appropriate option. We have reviewed all processing activities and only use consent as an option where the individual has a choice.

When reviewing the processing activity for compliance with the consent requirements, we ensure that none of the below are a factor: –

- Where we ask for consent but would still process it even if it was not given *(or withdrawn).* If we would still process the data under an alternative lawful basis regardless of consent, we recognise it is not the correct lawful basis to use;
- Where we ask for consent to process personal data as a precondition of a service we are offering, it is not given as an option and consent is not appropriate;
- Where there is an imbalance in the relationship, i.e. with employees.

11.1.4 INFORMATION PROVISIONS

Where personal data is obtained directly from the individual *(i.e. through consent, by employees, written materials and/or electronic formats (i.e. website forms, subscriptions, email etc*)), we provide the below information in all instances, in the form of a privacy notice: -

- The identity and the contact details of the controller and, where applicable, of the controller's representative;

- The contact details of our Centre Manager;
- The purpose(s) of the processing for which the personal information is intended;
- The legal basis for the processing;
- Where the processing is based on point (f) of Article 6(1) *"processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party"*, details of the legitimate interests;
- The recipients or categories of recipients of the personal data *(if applicable);*
- The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- The existence of the right to request access to and rectification or erasure of, personal data or restriction of processing concerning the Data Subject or to object to processing as well as the right to data portability;
- Where the processing is based on consent under points (a) of Article 6(1) or Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- The right to lodge a complaint with the Supervisory Authority;
- Whether providing personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the Data Subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
- The existence of any automated decision-making, including profiling, as referred to in Article 22(1) and (4) and explanatory information about the logic involved, as well as the significance and the envisaged consequences of such processing for the Data Subject;

The above information is provided to the Data Subject at the time the information is collected and records pertaining to the consent obtained are maintained and stored for eight years from the date of consent, unless there is a legal requirement to keep the information longer.

11.2 PRIVACY NOTICE

We define a Privacy Notice as a document, form, webpage or pop-up that is provided to individuals at the time we collect their personal data *(or at the earliest possibility where that data is obtained indirectly).*

Our Privacy Notice includes the Article 13 (*where collected directly from individual*) or *14 (where not collected directly)* requirements and provides individuals with all the necessary and legal information about how, why and when we process their data, along with their rights and obligations.

We have a link to our Privacy Notice on our website and provide a copy of physical and digital formats upon request. The notice is the customer facing policy that provides the legal information on how we handle, process and disclose personal information.

The notice is easily accessible, legible, jargon-free and is available in several formats, dependant on the method of data collection.

With lengthy content being provided in the privacy notice and with informed consent being based on its contents, we have tested, assessed and reviewed our privacy notice to ensure usability, effectiveness and understanding.

Where we rely on consent to obtain and process personal information, we ensure that it is: -

- Asks individuals to positively opt-in;
- Gives sufficient information to make an informed choice;
- Explains the different ways we will use the information;
- Provides a clear and simple way to indicate agreement to different types of processing.

Please see our Privacy Notice for more detail.

11.3 PERSONAL DATA NOT OBTAINED FROM THE DATA SUBJECT

Where we obtain and/or process personal data that has **not** been obtained directly from the Data Subject, we ensure that the information disclosures contain in Article 14 are provided to the Data Subject within 30 days of our obtaining the personal data *(except for advising if the personal data is a statutory or contractual requirement).*

In addition to the information disclosures in section 8.1.4, where personal data has not been obtained directly from a Data Subject, we also provide them with information about: -

- The categories of personal data;
- The source the personal data originated from and whether it came from publicly accessible sources.

Where the personal data is to be used for communication with the Data Subject, or a disclosure to another recipient is envisaged, the information will be provided at the latest, at the time of the first communication or disclosure.

Where we intend to further process any personal data for a purpose ***other*** than that for which it was originally obtained, we communicate this intention to the Data Subject prior to doing so and where applicable, process only with their consent.

Whilst we follow best practice in the provision of the information noted in the relevant section of this policy, we reserve the right not to provide the Data Subject with the information if: -

- They already have it and we can evidence their prior receipt of the information;
- The provision of such information proves impossible and/or would involve a disproportionate effort;
- Obtaining or disclosure is expressly laid down by Union or Member State law to which the Company is subject and which provides appropriate measures to protect the Data Subject's legitimate interest;
- Where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.

11.3.1 EMPLOYEE PERSONAL DATA

As per data protection laws, we do not use consent as a legal basis for obtaining or processing employee personal information. Employees are provided with appropriate information and training and are aware of how we process their data and why.

All employees are provided with a Staff Handbook and are provided with a Privacy Notice specific to the personal information we collect and process about them.

11.4 THE RIGHT OF ACCESS

We have ensured that appropriate measures have been taken to provide information referred to in Articles 13/14 and any communication under Articles 15 to 22 and 34 *(collectively, The Rights of Data Subjects*), in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

Such information is provided free of charge and is in writing, or by other means where authorised by the Data Subject and with prior verification as to the subject's identity *(i.e. verbally, electronic*).

Information is provided to the Data Subject at the earliest convenience, but at a maximum of 30 days from the date the request is received. Where the retrieval or provision of information is particularly complex or is subject to a valid delay, the period may be extended by two further months where necessary. However, this is only done in exceptional circumstances and the Data Subject is kept informed in writing throughout the retrieval process of any delays or reasons for delay.

Where we do not comply with a request for data provision, the Data Subject is informed within 30 days of the reason(s) for the refusal and of their right to lodge a complaint with the Supervisory Authority.

11.4.1 SUBJECT ACCESS REQUEST

Where a Data Subject asks us to confirm whether we hold and process personal data concerning him or her and requests access to such data; we provide them with: -

- The purposes of the processing;
- The categories of personal data concerned;
- The recipients or categories of recipient to whom the personal data have been or will be disclosed;
- If the Data has or will be disclosed to a third countries or international organisations and the appropriate safeguards pursuant to the transfer;
- Where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- The existence of the right to request rectification or erasure of personal data or restriction of processing of personal data concerning the Data Subject or to object to such processing;
- The right to lodge a complaint with a Supervisory Authority;
- Where personal data has not been collected by the Company from the Data Subject, any available information as to the source and provider;
- The existence of automated decision-making, including profiling and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the Data Subject.

Data Subject Access Requests (DSAR) are passed to the **Centre Manager** as soon as they are received and a record of the request is noted. The type of Personal Data held about the individual is checked against our Information Audit to see what format it is held in, who else has it has been shared with and any specific timeframes for access.

DSARs are always completed within 30-days and are provided free of charge. Where the individual makes the request by electronic means, we provide the information in a commonly used electronic

format, unless an alternative format is requested.

See the ***Data Subject Access Request Procedures*** policy document for more information.

11.5 DATA PORTABILITY

We provide all personal information pertaining to the Data Subject to them on request and in a format, that is easy to disclose and read. We ensure that we comply with the data portability rights of individuals by ensuring that, where technically feasible, all personal data is readily available and is in a structured, commonly-used and machine-readable format, enabling Data Subjects to obtain and reuse their personal data for their own purposes across different services.

To ensure that we comply with Article 20 of the data protection laws concerning data portability, we keep a commonly used and machine-readable format of personal information where the processing is based on: -

- Consent pursuant to point (a) of Article 6(1)
- Consent pursuant to point (a) of Article 9(2)
- A contract pursuant to point (b) of Article 6(1); and
- the processing is carried out by automated means

Where requested by a Data Subject and if the criteria meet the above conditions, we will transmit the personal data directly from us to a designated controller, where technically feasible.

All requests for information to be provided to the Data Subject or a designated controller are done so free of charge and within 30 days of the request being received. If for any reason, we do not act in responding to a request, we provide a full, written explanation within 30 days to the Data Subject or the reasons for refusal and of their right to complain to the supervisory authority and to a judicial remedy.

All transmission requests under the portability right are assessed to ensure that no other Data Subject is concerned. Where the personal data relates to more individuals than the subject requesting the data/transmission to another controller, this is always without prejudice to the rights and freedoms of the other Data Subjects.

11.6 RECTIFICATION & ERASURE

11.6.1 CORRECTING INACCURATE OR INCOMPLETE DATA

Pursuant to Article 5(d), all data held and processed by the Company is reviewed and verified as being accurate wherever possible and is always kept up to date. Where inconsistencies are identified and/or where the Data Subject or controller inform us that the data we hold is inaccurate, we take every reasonable step to ensure that such inaccuracies are corrected with immediate effect.

The Centre Manager is notified of the Data Subjects request to update personal data and are responsible for validating the information and rectifying errors where they have been notified. The information is altered as directed by the Data Subject, with the information audit being checked to ensure that all data relating to the subject is updated where incomplete or inaccurate. Once updated, we add an addendum or supplementary statement where applicable.

Where notified of inaccurate data by the Data Subject, we will rectify the error within 30 days and inform any third party of the rectification if we have disclosed the personal data in question to them. The Data Subject is informed in writing of the correction and where applicable, is provided with the details of any third-party to whom the data has been disclosed.

If for any reason, we are unable to act in response to a request for rectification and/or completion, we always provide a written explanation to the individual and inform them of their right to complain to the Supervisory Authority and to a judicial remedy.

11.6.2 THE RIGHT TO ERASURE

Also, known as *'The Right to be Forgotten'*, the Company complies as fully as is practically and legally possible with Articles 5.1(e) and 17 of the GDPR to ensures that personal data which identifies a Data Subject, is not kept longer than is necessary for the purposes for which the personal data is processed.

All personal data obtained and processed by us is categorised when assessed by the information audit and is either given an erasure date or is monitored so that it can be destroyed when no longer necessary.

11.7 THE RIGHT TO RESTRICT PROCESSING

There are certain circumstances where the Company restricts the processing of personal information, to validate, verify or comply with a legal requirement of a Data Subjects request. Restricted data is removed from the normal flow of information and is recorded as being restricted on the information audit.

Any account and/or system related to the Data Subject of restricted data is updated to notify users of the restriction category and reason. When data is restricted it is only stored and not processed in any way.

We will apply restrictions to data processing in the following circumstances: -

- Where an individual contest the accuracy of the personal data and we are in the process verifying the accuracy of the personal data and/or making corrections
- Where an individual has objected to the processing (*where it was necessary for the performance of a public interest task or purpose of legitimate interests*), and we are considering whether we have legitimate grounds to override those of the individual
- When processing is deemed to have been unlawful, but the Data Subject requests restriction as oppose to erasure
- Where we no longer need the personal data, but the Data Subject requires the data to establish, exercise or defend a legal claim

The Centre Manager reviews and authorises all restriction requests and actions and retains copies of notifications from and to Data Subjects and relevant third-parties. Where data is restricted, and we have disclosed such data to a third-party, we will inform the third-party of the restriction in place and the reason and re-inform them if any such restriction is lifted.

Data Subjects who have requested restriction of data processing are informed within 30 days of the restriction application and are also advised of any third-party to whom the data has been disclosed. We also provide in writing to the Data Subject, any decision to lift a restriction on processing. If for any reason, we are unable to act in response to a request for restriction, we always provide a written explanation to the individual and inform them of their right to complain to the Supervisory Authority and to a judicial remedy.

11.8 OBJECTIONS AND AUTOMATED DECISION MAKING

Data Subjects are informed of their right to object to processing in our Privacy Notices and at the point of first communication, in a clear and legible form and separate from other information. We provide opt-out options on all direct marketing material and provide an online objection form where processing is carried out online.

Individuals have the right to object to: -

- Processing of their personal information based on legitimate interests or the performance of a task in the public interest/exercise of official authority *(including profiling*)
- Direct marketing (*including profiling*)
- Processing for purposes of scientific/historical research and statistics

Where we process personal data for the performance of a legal task, in relation to our legitimate interests or for research purposes, a Data Subjects' objection will only be considered where it is on *'grounds relating to their particular situation'*. We reserve the right to continue processing such personal data where: -

- We can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual
- The processing is for the establishment, exercise or defence of legal claims

Where a Data Subject objects to data processing on valid grounds, the Company will cease the processing for that purpose and advise the Data Subject of cessation in writing within 30 days of the objection being received.

Where we use automated decision-making processes, we always inform the individual and advise them of their rights. We also ensure that individuals can obtain human intervention, express their point of view and obtain an explanation of the decision and challenge it.

12 OVERSIGHT PROCEDURES

12.1 SECURITY & BREACH MANAGEMENT

Alongside our *'Privacy be Design'* approach to protecting data, we ensure the maximum security of data that is processed, including as a priority, when it is shared, disclosed and transferred. Our ***Information Security Policies*** provide the detailed measures and controls that we take to protect personal information and to ensure its security from consent to disposal.

We carry out information audits to ensures that all personal data held and processed by us is accounted for and recorded, alongside risk assessments as to the scope and impact a data breach could have on Data Subject(s). We have implemented adequate and appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

Whilst every effort and measure are taken to reduce the risk of data breaches, the Company has dedicated controls and procedures in place for such situations, along with the notifications to be made to the Supervisory Authority and Data Subjects (where applicable).

13 TRANSFERS & DATA SHARING

We take proportionate and effective measures to protect Personal Data held and processed by us at all times, however we recognise the high-risk nature of disclosing and transferring personal data and as such, place an even higher priority on the protection and security of Data being transferred.

Data transfers within Ireland and the EU are deemed less of a risk than a third country or an international organisation, due to the data protection laws covering the former and the strict regulations applicable to all EU Member States.

Where Data is being transferred for a legal and necessary purpose, compliant with all Articles in the Regulation, we utilise a process that ensures such data is encrypted with a secret key and where possible is also subject to our data minimisation methods.

We use approved, secure methods of transfer and have dedicated points of contact with each Member State organisation with whom we deal. All Data being transferred is noted on our information audit so that tracking is easily available, and authorisation is accessible. The Centre Manager authorises all EU transfers and verifies the encryption and security methods and measures.

14 AUDITS & MONITORING

This policy and procedure document details the extensive controls, measures and methods used by us to protect personal data, uphold the rights of Data Subjects, mitigate risks, minimise breaches and comply with the data protection laws and associated laws and codes of conduct.

The Centre Manager has overall responsibility for assessing, testing, reviewing and improving the processes, measures and controls in place and reporting improvement action plans to the Board of Directors where applicable.

All reviews, audits and ongoing monitoring processes are recorded by the Centre Manager and copies provided to the Board of Management and are made readily available to the Supervisory Authority where requested.

Accountability Folder

An electronic folder will be maintained by our Centre Manager which collates all documents related to GDPR, including this policy document.

This folder will include but not be limited to:

- All policies and procedures put in place relating to GDPR and information security;
- Confidentiality agreements with Staff;
- Records of staff training and awareness;
- Processor contracts;
- Where processing on the basis of consent, records of this consent will be filed in hard copy format.

Demonstrating accountability also requires us to display information on data protection regulations in our reception area.

15 TRAINING

Through our strong commitment and robust controls, we ensure that all staff understand, have access to and can easily interpret the data protection laws requirements and its principles and that they have ongoing training, support and assessments to ensure and demonstrate their knowledge, competence and adequacy for the role.

Employees are continually supported and trained in data protection laws requirements and our own objectives and obligations around data protection.

16 PENALTIES

We understand our obligations and responsibilities under data protection laws and recognises the severity of breaching any part of the laws or Regulation. We respect the Supervisory Authority's authorisation under the legislation to impose and enforce fines and penalties on us where we fail to comply with the regulations, fail to mitigate the risks where possible and operate in a knowingly non-compliant manner.

Employees have been made aware of the severity of such penalties and their proportionate nature in accordance with the breach.

We recognise that: -

- Breaches of the obligations of the controller, the processor, the certification body and the monitoring body, are subject to administrative fines up to €10,000,000 or 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.
- Breaches of the basic principles for processing, conditions for consent, the Data Subjects' rights, the transfers of personal data to a recipient in a third country or an international organisation, specific processing situations (*Chapter IX*) or non-compliance with an order by the Supervisory Authority, are subject to administrative fines up to €20,000,000 or 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

17 RESPONSIBILITIES

We have voluntarily appointed a **Compliance Officer** ("CO") whose role it is to identify and mitigate any risks to the protection of personal data, to act in an advisory capacity to the Board of Directors and our employees and to actively stay informed and up-to-date with all legislation and changes relating to data protection. The CO is our Centre Manager, Laura Rowe.

The CO has overall responsibility for due diligence, privacy impact assessments, risk analysis and data transfers where personal data is involved and will also maintain adequate and effective records and management reports in accordance with the data protection laws and our own internal objectives and obligations.

Staff who manage and process personal or special category information will be provided with extensive data protection training and will be subject to continuous development support and mentoring to ensure that they are competent and knowledge for the role they undertake.