# Data Protection by Design and by Default policy

## Introduction, scope and purpose

This policy is to outline the commitment the practice has to the concept of "Data Protection by Design and by Default" and it's role in ensuring that the practice upholds it's requirement to ensure that all data processing it is responsible for is in compliance with the Principles of GDPR, as articulated in Article 5 of GDPR (paraphrased below):

1. . Personal data shall be:
    1. processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
    2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation');
    3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
    4. accurate and kept up to date to ensure that any inaccurate personal data is erased or rectified without delay ('accuracy');
    5. kept for no longer than is necessary for the purposes for which the personal data are processed ('storage limitation');
    6. processed in a manner that ensures appropriate, including protection against unauthorised or unlawful processing, against accidental loss, destruction or damage ('integrity and confidentiality').
2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

As part of the practice's compliance as a Data Controller with data protection legislation, we actively pursue a policy of Data Protection by Design and by Default for all data processing activities we undertake, including the core medical services we provide.

Data Protection by Design and by Default is a key element underpinning the principles of GDPR and is articulated under Article 25 of GDPR as follows:

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures[1], such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

2.

    I. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed.

    II. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.

    III. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

[1] For the purposes of Article 25, "appropriate technical and organisational measures" are defined under Recital 78 of GDPR as:

- The protection of the rights and freedoms of natural persons with regard to the processing of personal data require that appropriate technical and organisational measures be taken to ensure that the requirements of this Regulation are met.
- In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default.
- Such measures could consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features.
- When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations.
- The principles of Data Protection by Design and by Default should also be taken into consideration in the context of public tenders.

**Policy Statements**

In practice, this Article of the GDPR covers a multitude of issues designed to ensure that organisations evaluate Data Protection and Privacy as core considerations for any proposed or existing data processing, and to ensure that any solution used supports these considerations.

As part of our compliance we ensure that (inter alia):

- We take a proactive, not reactive, approach to Data Protection by Design and by Default to ensure that Data Protection and Privacy are primary considerations.
- We consider data protection and privacy as part of the implementation of our medical services and business practices.
- We consider carrying out Data Protection Impact Assessments for any new data processing or data sharing activities we are considering
- We ensure that data protection and privacy are an essential component of the functionality of our processing systems.
- We endeavour to anticipate potential privacy risks before they occur, and take steps to prevent harm to individuals.
- We only process the personal data that we specifically need for our purposes, and do not process or collect data unless it is required for this purpose.
- We will only use personal data for the purpose for which we collect it (unless another purpose is evaluated and deemed compatible).
- If required for non direct care uses, all identifiable data will be de-identified by pseudonymisation or anonymisation techniques to an appropriate standard that is in compliance with all relevant legislation
- We ensure that personal data is automatically protected in any IT system or business practice, so that individuals should not have to take any specific requests to protect their privacy.
- We provide the identity and contact information of those responsible for data protection to individuals.
- We adopt a ‘plain language’ policy for documentation so that individuals can easily understand what we are doing with their personal data and how that data should be managed.
- We provide individuals with information such as privacy notices so they can determine how we are using their personal data, and whether our policies are being properly enforced.

- We offer strong privacy as a default and respect individual preferences, wherever possible,  for how data is used.
- We only use data processors that provide robust guarantees of their own technical and organisational measures for securely processing individual's data.
- When we use other systems or products in our processing activities, we make sure that we only use those whose designers and manufacturers have taken data protection issues into account.
- We use privacy-enhancing technologies whenever applicable to assist us in complying with our data protection by design obligations.
- We have comprehensive polices and procedure in place regarding Data Protection and Privacy, and these polices are adhered to, and adherence is monitored and reviewed