DATA PROTECTION POLICY UNDER EXCLUSIVE LICENCE OF LOGIC DOCUMENT LICENCE PERIOD: MAY 2018 – APRIL 2019 REVIEW: APRIL 2019

Article 24 of the G.D.P.R regulation states that in relation to the collection, collation, processing and sharing of data, measures need to be implemented appropriately as defined by the Data Protection Policies by the controller and processor.
This policy must be concise to the business at hand and easy for the consumer to understand. This covers a variable between protections for the consumer with adding productivity to services offered.
The General Data Regulation 2016 implementation 2018 replaces EU Data Protection Directives 1995 and supersedes the laws of individual member states that were developed in compliance with the Data Protection Directive. Its purpose is to protect the rights and freedoms of natural persons and to ensure personal data is not processed without their knowledge, and wherever possible it is processed with their consent.
Ailgynnau Consulting Limited will apply the Logic Document Data Protection Policy for G.D.P.R legislation to the processing of personal data wholly or partly by automated means and to the processing other than automated means of personal data that form part of a filing system, marketing system, CRM system or for any other reason not defined in an engagement supplied by Ailgynnau Consulting Limited.
Any information relating to an identified or identifiable person or data subject directly or indirectly, in particular by reference to the identifier such as: name, ID Number, location data, business, position held or to one or more specific to the physical, physiological, genetic, mental, economical, cultural or social identity including revealing racial or ethnic origin. Political opinion, religious or philosophical beliefs, trade union or paid memberships to networking organisations and affiliated service and the collecting and processing of data that can be used for identifying a data subject with reference to the following data concerning health, or data concerning a data subjects sex life or sexual orientation.

LOGIC DOCUMENT

This statement and policy under licence from Logic Document includes the holding, obtaining, recording, use, disclosing, sharing and the storage of data.
The General Data Protection Regulations (GDPR), which came into force on 25 May 2018, completely overhauls the data protection regime governed by the Data Protection Directive and supersedes the Data Protection Act 1998 (DPA) upon which it was based. GDPR extensively updates the definition of identifiable information.
Table of contents

Ailgynnau Consulting Limited needs to collect person-identifiable information about individuals to carry out its functions and fulfil its objectives. Personal data is defined as 'information which relates to a living individual and from which they can be identified, either directly or indirectly'. Personal data at Ailgynnau Consulting Limited can include employees (present, past and prospective), patients, contractors and third parties, private and confidential information as well as sensitive information, whether in paper, electronic or other form Irrespective of how information is collected, recorded and processed person identifiable information must be dealt with properly to ensure compliance with the Data Protection Act (DPA) 1998 and the General Data Protection Regulations (GDPR). The DPA requires Ailgynnau Consulting Limited to comply with the Data Protection Principles and to notify the Information Commissioner about the data that we hold and why we hold it. This is a formal notification and is renewed annually. The DPA gives rights to data subjects (people that we hold information about) to access their own personal information, to have it corrected if wrong, in all permitted circumstances to ask us to stop using it and to seek damages where we are using it improperly. The lawful and correct treatment of person-identifiable information by Ailgynnau Consulting Limited is paramount to the success of the organisation and to the consumer to maintain the confidence of its service users and employees. This policy will help Ailgynnau Consulting Limited ensure that all person-identifiable information is handled and processed lawfully and correctly.

Data Protection Act and GDPR principles

Ailgynnau Consulting Limited has a legal obligation to comply with all relevant legislation in respect of data protection and information / IT security. The organisation also has a duty to comply with guidance issued by the ICO, as well as other relevant guidance issued by advisory groups and professional bodies. All legislation relevant to an individual's right to the confidentiality of their information and the ways in which that can be achieved and maintained are paramount to Ailgynnau Consulting Limited. Significant penalties can be imposed upon the organisation for non- compliance. The aim of this policy is to outline how Ailgynnau Consulting Limited meets its legal obligations in safeguarding confidentiality and adheres to information security standards. The obligations within this policy are principally based upon the requirements of the Data Protection Act 1998 and GDPR, as the key legislative and regulatory provisions governing the security of person- identifiable information.

What information is covered?

Personal data within the respective legislative and regulatory provisions covers 'any data that can be used to identify a living individual either directly or indirectly'. Individuals can be identified by various means including but not limited to, their address, telephone number or e-mail address. Anonymised or aggregated data is not regulated by the provisions, providing the anonymisation or aggregation of the data is irreversible.

Policy statement:

This document defines the data protection policy for Ailgynnau Consulting Limited. It applies to all person-identifiable information obtained and processed by the organisation and its employees. It sets out: the organisations policy for the protection of all person-identifiable information that is processed, establishes the responsibilities (and best practice) for data protection, references the key principles of the Data Protection Act 1998 and GDPR.

Principles:

Principles and the objective of this policy is to ensure the protection of Ailgynnau Consulting Limited information in accordance with relevant legislation.

To ensure notification;

Annually notify the Information Commissioner about Ailgynnau Consulting Limited use of person- identifiable information.

To ensure professionalism;

All information is obtained, held and processed in a professional manner in accordance with the principles of the Data Protection Act 1998 and the provisions of GDPR.

To preserve security;

All information is obtained, held, disclosed and disposed of in a secure manner.

To ensure awareness;

Provision of appropriate training and promote awareness to inform all employees of their responsibilities.

Data Subject access;

Prompt and informed responses to subject access requests. The policy will be reviewed periodically by Ailgynnau Consulting Limited DPO TEAM namely Logic Document. Where review and update are necessary due to legislative changes this will be done immediately. In accordance with the Logic Documents equality and diversity policy statement, this procedure will not discriminate, either directly or indirectly, on the grounds of gender, race, colour, ethnic or national origin, sexual orientation, marital status, religion or belief, age, union membership, disability, offending background or any other personal characteristic.

Scope of this policy;

This policy will ensure that person-identifiable information is processed, handled, transferred, disclosed and disposed of lawfully. Person-identifiable information should be handled in the most secure manner by authorised staff only, on a need to know basis. The procedures cover all person identifiable information whether clinical or nonclinical, electronic or paper which may relate to patients, employees, contractors, consumers and third parties about whom we hold information.

Policy

Ailgynnau Consulting Limited obtains and processes person-identifiable information for a variety of different purposes, including but not limited to: staff records and administrative records, matters relating to the prevention, detection and investigation of fraud and corruption from employees of Ailgynnau Consulting Limited. Complaints and requests for information, such information may be kept in either computer or manual records. In processing such personal data, Ailgynnau Consulting Limited will comply with the data protection principles within the Data Protection Act 1998 and GDPR LEGISLATION MAY 2018.

Data protection responsibilities: Overall responsibilities;

Ailgynnau Consulting Limited Board members, collectively known as the ‘data controller’ permit the organisation’s staff to use computers and relevant filing systems (manual records) in connection with their duties. Ailgynnau Consulting Limited Board members and Logic Document have legal responsibility for the notification process and compliance of the Data Protection Act 1998 and GDPR breach reporting policies and

legislation. Ailgynnau Consulting Limited Board members whilst retaining their legal responsibilities have delegated data protection compliance to the Data Protection Officer Namely Logic Document, whose responsibilities have been allocated to the organisation's Information Governance, Risk management and due diligence compliance reports. The Data Protection Officer's responsibilities include: ensuring that the policy is produced and kept up to date, ensuring that the appropriate practice and procedures are adopted and followed by Ailgynnau Consulting Limited. Provide advice and support to the Board on data protection issues within the organisation.
Work collaboratively with Organisational Development and Governance and Assurance to help set the standard of data protection training for staff, ensure data protection notification with the Information Commissioner's Office is reviewed, maintained and renewed annually for all use of person identifiable information, ensure compliance with individual rights, including subject access requests, act as a central point of contact on data protection issues within the organisation, implement an effective framework for the management of data protection.

Line manager's responsibilities:

All managers across the organisation are directly responsible for: ensuring their staff are made aware of this policy and any notices. Ensuring staff are aware of their data protection responsibilities. Ensuring staff receive suitable data protection training.

General responsibilities:

All Ailgynnau Consulting Limited employees, including temporary and contract staff are subject to compliance with this policy. Under GDPR, individuals and Directors can be held personally liable for data protection breaches if compliance training is not provided and administered from a designated DPO namely Logic Document. Ailgynnau Consulting Limited employees have a responsibility to inform the Data Protection Officer, namely Logic Document of any new use of personal data, as soon as reasonably practicable after it has been identified. All Ailgynnau Consulting Limited employees will, on receipt of a request from an individual for information held, known as a subject access request or concerns about the processing of personal information, immediately notify the DPO, namely Logic Document who will inform the ICO and engage with the data subject in the agreed time set out in accordance with this policy.

Monitoring:

Compliance with this policy will be monitored by Logic Documents Governance team, together with internal audit reviews where necessary. The Information Governance and Risk Management Lead, namely Logic Document is responsible for the monitoring, revision and updating of this policy document on an annual basis or sooner, should the need arise.

Validity of this policy:

This policy will be reviewed at least annually under the authority of Logic Document. Associated data protection standards will be subject to an ongoing development and review programme.
Data Protection Act 1998 – Data protection principles:
1. Personal data shall be processed fairly and lawfully.
2. Personal data shall be obtained for one or more specified and lawful purposes and shall not be

further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.
Summary of relevant legislation and guidance General Data Protection Regulations (GDPR) A legal basis must be identified and documented before personal data can be processed. 'Controllers' and 'Processors' will be required to document decisions and maintain records of processing activities.
Human Rights Act 1998 This Act binds public authorities including Health Authorities, Trusts and Primary Care Groups to respect and protect an individual's human rights. This will include an individual's right to privacy (under Article 8) and a service user's right to expect confidentiality of their information always. Article 8 of the Act provides that "everyone has the right to respect for his private and family life, his home and his correspondence". However, this article also states, "there shall be no interference by a public authority with the exercise of this right except as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety, or the economic well-being of the country, for the prevention or disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others". Each organisation must act in a way consistent with these requirements. It must take an individual's rights into account when sharing personal information about them.
Freedom of Information Act 2000: This Act gives individuals rights of access to information held by public authorities.
Regulation of Investigatory Powers Act 2000: This Act combines rules relating to access to protected electronic information as well as revising the "Interception of Communications Act 1985". The aim of the Act was to modernise the legal regulation of interception of communications, in the light of the Human Rights laws and rapidly changing technology.
Crime and Disorder Act 1998 This Act introduces measures to reduce crime and disorder, including the introduction of local crime partnerships around local authority boundaries to formulate and implement strategies for reducing crime and disorder in that local area. The Act allows disclosure of person-identifiable information to the Police, Local Authorities, Probation Service or the Health Service but only if the purposes are defined within the Crime and Disorder Act. The Act does not impose a legal requirement to disclose person identifiable information and responsibility for disclosure rests with the organisation holding the information.
The Computer Misuse Act 1990:
This Act makes it a criminal offence to access any part of a computer system, programs

and/or data that a user is not entitled to access Ailgynnau Consulting Limited will issue each employee with an individual user id and password which will only be known to the individual and must not be divulged to other staff. This is to protect the employee from the likelihood of their inadvertently contravening this Act Ailgynnau Consulting Limited will adhere to the requirements of the Computer Misuse Act 1990, by ensuring that its staff are aware of their responsibilities regarding the misuse of computers for fraudulent activities or other personal gain. Any member of staff found to have contravened this Act will be considered to have committed a disciplinary offence and be dealt with accordingly.
The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 This Act allows employers to intercept and record communications in certain prescribed circumstances for legitimate monitoring, without obtaining the consent of the parties to the communication.
Information Security Management: Logic Document will provide under the licence Code of Practice. The guidelines provide a framework for consistent and effective information security management that is both risk and standards-based and is fully integrated with other key sharing Information Governance areas. Without effective security, referral information assets may become unreliable and untrustworthy, may not be accessible where or when needed, or may be compromised by unauthorised third parties.
Confidentiality: Logic Documents Code of Practice gives guidance concerning the required practice for those who work within or under contract to referral organisations concerning confidentiality and patients' consent to the use of their personal data.

.