Innatus Digital Data Protection Policy

Definitions

- **Personal Data** means data consisting of information which relates to a living individual who can be identified from that information (or from that and other information in the possession of the data user), including any expression of opinion about the individual, but not any indication of the intentions of the data user in respect of the individual.
- **Sensitive Personal Data** refers to five sub-sets of personal data, being:
    - information on an individual's racial or ethnic origins
    - information on an individual's physical, mental or sexual life
    - information on an individual's criminal activities and convictions
    - information on an individual's political or religious opinions or beliefs
    - information on any trade union membership held by the individual
- **Data Controller** refers to the company, organisation or individual responsible for the Personal Data and which is responsible for the manner in which the personal data is processed.
- **Data Processor** refers to any company, organisation or individual who processes personal data on behalf of the Data Controller.
- **Processing** refers to any activity that can be done with or applied to personal data, including its acquisition, organisation, storage, retrieval, consultation, amendment, availability, disclosure, erasure or destruction.

Scope

This Data Protection Policy shall apply to all Personal Data acquired, received, processed, stored, amended, disclosed and erased by Innatus Digital. This shall include Company data and personal data owned by an external organisation and entrusted to the Company under a contract that specifically communicates data protection requirements.

This Data Protection Policy shall be communicated to all employees, contractors, third-party users, external Data Processors, and any other organisation or individual with a bonafide need to access Personal Data held by Innatus Digital.

Policy

As a Data Controller, Innatus Digital shall comply with the eight data protection principles as detailed within Schedule 1 of the Data Protection Act 1998:

- **First principle**: personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless at least one of the “conditions for processing” has been met (or one of the “conditions for processing sensitive data” has been met for sensitive personal data.
- **Second principle**: personal data shall be obtained only for one or more specified and lawful purposes. They shall not be further processed in any manner incompatible with the purpose of those purposes.
- **Third principle**: personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- **Fourth principle**: personal data shall be accurate and, where necessary, kept up to date.
- **Fifth principle**: personal data processed for any purpose or purposes shall not be kept longer than is necessary for that purpose or those purposes.
- **Sixth principle**: personal data shall be processed in accordance with the rights of the data subject under the Data Protection Act 1998.
- **Seventh principle**: appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and accidental loss or destruction of, or damage to, personal data.
- **Eighth principle**: 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.

In addition:

- Innatus Digital will allow any company or individual to dictate how their data is used; any impact this has on the services we can offer you will be clearly communicated.
- Innatus Digital shall ensure that it maintains an accurate registration with the Office of the Information Commissioner, including all appropriate “purposes” for which data is to be processed. Such “purposes” shall be reviewed annually, at the point of registration renewal, or at any point during the year where changes indicate that the purposes need to be changed.
- Innatus Digital shall comply with the “Right of Access to Personal Data” requirements as detailed within the Act. This shall include the following:

    - Acknowledging all written requests to the Company from individuals seeking details of personal data that may be held about them.
    - Subject to receipt of the current processing fee and sufficient detail from the individual to allow both the authentication of their identity and the identification of any personal data that may be held about them, details of such personal data shall be provided in writing within *(insert number of days).*
    - Full and prompt cooperation with any Order a Court of Law issues.
- Innatus Digital shall ensure that risks to personal data are identified during the periodic review of risk assessments and appropriate controls implemented to ensure that the eight principles of the Act can be fully complied with at all times.
- Innatus digital will ensure that any marketing emails are fully compliant with this policy and the law.
- Innatus Digital shall ensure that any actual or potential loss, theft or another form of breach is promptly reported internally, as well as being reported to the appropriate external authority.

Responsibilities

The *Managing Director* shall be responsible for:

- Co-ordinating activities relating to data protection within Company
- Ensuring timely and accurate registration as required by the Act
- Assisting in the investigation of any actual or potential personal data breaches
- Advising the Company on changes to data protection legislation
- Co-ordinating the response to any individual personal data requests received
- Providing data protection training to all persons within the Scope of this Policy

All employees, contractors, and third parties, as defined within the Scope of this Policy, shall comply with all requirements of this Data Protection Policy and take all possible steps to ensure that their processing of personal data (as defined in Section 2.0) is undertaken in strict accordance with the Data Protection Act 1998 and this Data Protection Policy. Failure to adhere to this Policy shall result in disciplinary action being taken.

Review

This Policy needs to be formally reviewed on an annual basis, as a minimum, or if required changes are identified to address one or more of the following:

- A change in business activities, which will or could possibly affect the current operation of the Company Information Security Management System, and the relevance of this document
- A change in the manner in which the Company manages or operates its information assets and/or their supporting assets, which may affect the accuracy of this document
- An identified shortcoming in this Policy's effectiveness due to a reported information security incident, formal review or an audit finding.