Data Protection Policy

Data Protection

Synergic UK Ltd takes its responsibilities with regard to the management of the requirements of the Data Protection Act 1998 very seriously. This document provides the policy framework through which effective management of Data Protection matters can be achieved.

1. Scope of the Policy

The purpose of this policy is to ensure that the Company and the Company's staff comply with the provisions of the Data Protection Act 1998 when processing personal data. Any serious infringement of the Act will be treated seriously by the Company and may be considered under disciplinary procedures.

The Company expects all of its staff to follow the ethical behaviours commensurate with broader public sector principles such as Caldicot. Those are: selflessness, integrity, objectivity, accountability, openness, honesty and leadership. These Principles underlie the Company's Ethical Framework and are incorporated into this policy.

This policy applies regardless of where the data is held, ie if it is held on personally-owned equipment or outside Company property.

The Company is required to adhere to the eight principles of data protection as laid down by the Act. In accordance with those principles personal data shall be:

- Processed fairly and lawfully
- Processed for specified purposes only
- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept longer than necessary
- Processed in accordance with data subjects' rights
- Processed and held securely
- Not transferred outside the countries of the European Economic Area without adequate protection.

2. Responsibilities

1. Company responsibilities as the Data Controller the Company is responsible for establishing policies and procedures in order to comply with the requirements of the Data Protection Act 1998.

2. Governance Team responsibilities. The Governance Team holds responsibility for
    - the Company's Data Protection notification.
    - Details of the Company's notification that are published on the Information Commissioner's website.
    - Anyone who is, or intends, processing personal data for purposes not included in the notification should seek advice from the Governance Team;
    - drawing up guidance, giving advice and promoting compliance with this policy in such a way as to ensure the easy, appropriate and timely retrieval of information;
    - the appropriate compliance with subject access rights and ensuring that data is released in accordance with subject access legislation under the Data Protection Act 1998;
    - ensuring that any data protection breaches are resolved, catalogued and reported appropriately in a swift manner and in line with guidance from the Information Commissioner's Office;
    - investigating and responding to complaints regarding data protection including requests to cease processing personal data.

3. Staff responsibilities
    - Staff members who process personal data about subcontractors, staff, applicants, alumni or any other individual must comply with the requirements of this policy.
        - Staff members must ensure that:
        - all personal data is kept securely;
        - no personal data is disclosed either verbally or in writing, accidentally or otherwise, to any unauthorised third party;
        - personal data is kept in accordance with the Company's retention schedule;
        - any queries regarding data protection, including subject access requests and complaints, are promptly directed to the Governance Team;
        - any data protection breaches are swiftly brought to the attention of the Governance Team and that they support the Governance Team in resolving breaches;
        - where there is uncertainty around a Data Protection matter advice is sought from the Governance Team. When members of staff are responsible for supervising subcontractors doing work which involves the processing of personal information(for example in research projects), they must ensure that those sub-contractors are aware of the Data Protection Principles, in particular, the requirement to obtain the data subject's consent where appropriate.

- Staff who are unsure about who are the authorised third parties to whom they can legitimately disclose personal data should seek advice from the Governance Team.

4. Third-Party Data Processors
    - Where external companies are used to process personal data on behalf of the Company, responsibility for the security and appropriate use of that data remains with the Company.

      Where a third-party data processor is used:
        - a data processor must be chosen which provides sufficient guarantees about its security measures to protect the processing of personal data; reasonable steps must be taken that such security measures are in place;
        - a written contract establishing what personal data will be processed and for what purpose must be set out;
        - a data processing agreement, available from the Governance Team, must be signed by both parties.
        - For further guidance about the use of third-party data processors please contact the Governance Team.

5. Contractors, Short-Term Staff
    - The Company is responsible for the use made of personal data by anyone working on its behalf. Managers who employ contractors, short term or voluntary staff must ensure that they are appropriately vetted for the data they will be processing. In addition managers should ensure that:
        - any personal data collected or processed in the course of work undertaken for the Company is kept securely and confidentially;
        - all personal data is returned to the Company on completion of the work, including any copies that may have been made. Alternatively that the data is securely destroyed and the Company receives notification in this regard from the contractor or short term / voluntary member of staff;
        - the Company receives prior notification of any disclosure of personal data to any other organisation or any person who is not a direct employee of the contractor;
        - any personal data made available by the Company, or collected in the course of the work, is neither stored or processed outside the UK unless written consent to do so has been received from the Company;
        - all practical and reasonable steps are taken to ensure that contractors, short term or voluntary staff do not have access to any personal data beyond what is essential for the work to be carried out properly.

3. Data Protection breaches

Where a Data Protection breach occurs, or is suspected, it should reported immediately in accordance with the Data Security Breach Incident Management Policy which states:

Confirmed or suspected data security breaches should be reported promptly to the IT Service Desk as the primary point of contact on email: operations@synergic.co.uk. The report should include full and accurate details of the incident including who is reporting the incident and what classification of data is involved.

4. Contact

Queries regarding this policy or the Data Protection Act at large should be directed to the Governance Team at operations@synergic.co.uk