DATA PROTECTION POLICY

Introduction

Antrec Limited (Antrec) not only intends to comply with its legal obligations under the Data Protection Act 1998 (The Act), but also wishes to assure both employees and all other persons about whom it retains personal data, that this will be processed in compliance with The Act and will be stored in a secure, confidential and appropriate manner. The data will only be stored whilst relevant and will not be disclosed to any person without the individual's personal written authority or unless required by law.

The Data Protection Act

The DPA relates to any personal data (any information by which an individual can be identified) held by any agency. The Act sets out the conditions by which such information can be obtained and retained as well as an individuals' right of access to such data. The Act relates only to living individuals.

The 8 principles relating to the storage of information:

- Fairness and Legality – personal data must be processed fairly and lawfully. Nobody should be deceived or misled about the purpose for which their data is to be processed
- Purpose – personal data can only be obtained for specified and lawful purposes with the permission from the data subject and should only be used for its original purpose
- Adequacy – personal data has to be adequate, relevant and not excessive in relation to the purpose for which the data is meant to be processed. You cannot collect information that you do not need
- Accuracy – personal data should be accurate and up-to-date and should be amended if it's found to be incorrect
- Length of Use – the Act requires that personal data is not kept any longer than is necessary for the purpose it was obtained. It cannot be used for anything else or passed on more widely without the individual's consent
- Access rights – data subjects have the right to access their personal data and can block any processing that causes or is likely to cause them distress. They can insist that their data is not used for marketing purposes and they have the right to know the rule behind any automated decision-making process
- Security – the Act requires organisations to take all appropriate measures to prevent unauthorised processing or personal data against loss, damage or destruction. This extends to third party processors
- Transfer outside the EU – personal data cannot be transferred to a country outside the EU unless that country has in place a level of data protection comparable to that of the EU

The Data Protection Act 1988 gives all individuals who are the subject of personal data a general right of access to the data that relates to them. These are known as 'subject access rights'. In most cases it is expected that information will be supplied within 40 days of a request being made.

Information held under the DPA can be shared between colleagues within the same agency but can only be shared with those from another agency if:-

- The consent of the subject has been obtained first
- There is a pressing need under other legislation (i.e. the Children Act)

Responsibilities

The person responsible for ensuring the maintenance, regular review and updating of this policy is the Managing Director. Individual Line Managers are then responsible for ensuring that this policy is applied in their own area. Any queries on the application or interpretation should be discussed with either the Managing Director or the Data Protection Officer.

Personal Data

Personal data is any information, whether held on a computer system or in an organised paper based filing system which, either on its own or in conjunction with other information held about a person enables Antrec to identify that person. The types of personal data Antrec will collect about employees may include any or all of the following: name and address; contact details; next of kin details; date of birth; education and qualifications; bank account details; salary information; performance ratings; training records and details of positions held within Antrec.

In addition to the examples given above Antrec may also store or process sensitive personal data. This is defined as information relating to, for example employees' racial or ethnic origin, or their physical or mental health.

Consent to Process Data

Antrec will only collect personal information about employees or clients when the information is required for a legitimate business or legal reasons. Under normal circumstances personal data will only be obtained from the employee or client or with his/her consent. Where it is appropriate to consult sources other than the data subject (e.g. for references) then he/she will be informed of that fact.

Sensitive personal data may only be processed if, in addition, to the above, a sensitive personal data condition is met:

- The data subject has given his/her explicit consent to processing; or
- The processing is necessary for the performance of any right or obligation imposed by law, this includes data processed to:
  - Ensure workers' health & safety and welfare at work;
  - Keep a safe working environment;
  - Prevent discrimination on the grounds of race, sex or disability;
  - Consider DDA reasonable adjustments to the workplace;
  - Maintain records e.g. SMP and SSP;
  - Prevent unfair dismissal of workers;
  - Supply information on accidents if there may be a claim for industrial injuries benefit;
  - Protect property or funds belonging to customers but in the employer's possession;
  - Ensure continuity of employment following a TUPE transfer.
- The processing is necessary to protect vital interests; or
- The information has been made public; or
- The processing is necessary for the administration of justice; or
- The processing is necessary for medical purposes; or
- The processing is for equal opportunities monitoring.
- The processing is for reporting outcomes to SFA/EFA/ESF/DWP and other relevant prime contract holders and monitoring the effectiveness of our service; or
- The processing is for supporting clients to move into employment/training.

Disclosure of Employee Personal Data

Antrec may disclose employee's personal data to reputable third parties such as HM Revenue & Customs; pension schemes and healthcare providers in order to carry out the above purposes. However, other than as set out above the Company will not disclose or share your personal data to third parties without your permission, unless this is necessary for the for the purposes of your employment or as required by law.

Disclosure of Client Personal Data

Antrec is required contractually to disclose client personal data to SFA, EFA & ESF or our contract holder to monitor the effectiveness of our service and report outcomes. In addition we may share data with employers and other third party organisations for the purposes of helping client's gain skills and move into sustainable work. However, other than as set out above the Company will not disclose or share client personal data to employers and other third parties without permission, unless this is required by law.

Access to Personal Data

The Company will keep your personal data for so long as is required by law, or as is relevant for the purposes for which it was collected. During this period an employee or client may make a request to be given access to such data that is held about them.

For employees such an application should be made to HR who will advise of the process for making a formal subject access request.

For clients a written request should be made to either the Data Protection Officer or the Head of Department

The Company reserves the right to make a charge for this, up to a maximum of £10. Where any personal data held about you is inaccurate, an employee or client may request that it be corrected, updated, supplemented or deleted.

Client and Third Party Personal Data

As an employee of Antrec you will work and deal with personal data relating to clients; such as address details; billing records, credit card details etc. Clients' personal data must be respected at all times and must not be disclosed or used other than for legitimate business purposes.

Employees are responsible for:

- Ensuring that any personal data provided to the Company is accurate.
- Promptly updating HR of any changes to personal data in order that records may be updated accordingly.
- When making a subject access request to assist the Company in identifying the personal data which is being requested.
- Taking care of personal data relating to clients or colleagues, not disclosing this to third parties unless authorised or required to do so.
- Ensuring that client and third party information is collected, recorded and used in accordance with the principles of the Data Protection Act.

Managers are responsible for:

- Ensuring that employee data is acquired and stored in accordance with the data protection principles e.g. in secure filing systems or password protected in the case of electronic data.
- Not disclosing employee data inappropriately to third parties i.e. without a legitimate reason and without the employee's consent.
- Ensuring that employees who are dealing with clients or other third party data are aware of their responsibilities.
- Dealing with any subject access requests from employees – in the first instance any employee should be referred to HR.

The Senior Management Team are responsible for:

- Advising and guiding Managers on how to deal with any breach of the rules and procedures identified in this policy.
- Responding to any queries on the application or interpretation of this policy.
- Maintaining, reviewing and updating this policy.