DATA PROTECTION POLICY

Andante Project Resources Ltd trading as Avril Chaffey PR

Date of adoption: March 2018
Date of next review: March 2019

Version	Date	Description	Changes	Author
0	26/02/2018	Original Document	N/A	P Chaffey, A Chaffey

Introduction

1. Andante Project Resources Ltd (APR) is committed to compliance with all relevant legislation in respect of personal data, and to protecting the rights and privacy of individuals whose information APR collects in accordance with the Data Protection Act 1998 (DPA) and the General Data Protection Regulation (GDPR).

2. Data protection is the responsibility of the Directors of APR to make sure that they are compliant. This policy has been approved by the Directors and it will be reviewed on a regular basis.

3. The DPA establishes eight data protection principles which govern the processing of personal data. These state that personal data must be:

   - Processed fairly and lawfully
   - Obtained for one or more specified and lawful purposes
   - Adequate, relevant and not excessive
   - Accurate and up-to-date
   - Not kept for longer than is necessary
   - Processed in accordance with the rights of data subjects
   - Kept securely
   - Not transferred out of the European Economic Area without adequate protection

The Data Protection Act 1998 & GDP Regulations

1. The DPA & GDPR established a framework of rights and duties which are designed to safeguard personal data. It places legal obligations on organisations which handle personal data about individuals.

2. The DPA & GDPR applies to all electronic records and also to some paper-based records if they form part of a relevant filing system. In practice this relates to filing systems which are organised in a manner where documents relating to a living individual can be found easily – for example where files are ordered by name and alphabetically.

Definitions used by APR (drawn from the DPA where applicable)

Data Controller	Any person or organisation that makes decisions with regard to particular personal data including decisions regarding the purposes for, and the way in which, personal data is processed.
Data Subject	Any living individual who is the subject of personal information held by an organisation.
Personal Data	Data relating to a living individual can be identified from that data such as name, telephone number, email address. It also includes • Information that enables someone to "recognise" an individual such as accents, key phrases or situations. • Data that is likely to come into the possession of APR. • Any expression of opinion about the individual or any indication of the intentions of APR in respect of the individual.
Sensitive Personal Data	The DPA also classifies certain types of personal data as "sensitive". The presumption is that, because information about these matters could be used in a discriminatory way, and is likely to be of a private nature, it needs to be treated with greater care than other personal data. Sensitive personal data is defined as personal data consisting of information as to: • Racial or ethnic origins • Political opinions • Religious beliefs or other beliefs of a similar nature • Trade Union membership • Physical or mental health or condition • Sexual life • The commission or alleged commission of any offence, or any proceedings for any offence committed or alleged to have been committed
Data Processing	Processing, in relation to personal data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data.
Subject Access Request	A request from an individual to see any personal data that APR holds on him/her

3. APR from time to time obtains and processes personal data relating to its clients employees. Its procedures are designed to comply with the Data Protection Principles highlighted in the introduction above.

Processing Personal Data

1. APR processes personal data relating to client's employee's working history for the following purposes:

    - To produce press releases and articles for publication in Trade and local press including online magazines.

2. All press releases and articles are subject to sign off approval procedure before issuing to any organisation, editor or journalist to ensure they are an accurate reflection of the facts.

3. APR obtains consent to process the personal data provided by individuals.

4. With regard to Information Sharing, as identified above and due to the nature of its business APR share's some clients employees personal data relating to work history with the other press organisations .

Processing Employee Data

Andante Project Resources Ltd has no employees.

Privacy Notices

APR ensures that all documentation used to collect personal data with regard to its clients employees complies with "fair collection" requirements of the DPA and GDPR. A privacy statement is available on request.

Data Retention

1. APR has established a data retention schedule which identifies retention periods for the personal data held.

2. It has also set up a system for ensuring that the relevant retention limit is observed in practice, and for documenting and reviewing the retention policy. Personal data will be disposed of in a secure manner.

The Rights of Subject Access

APR has a Subject Access Requests Procedure as identified below:

- Subject access requests must be put in writing

- Data subjects must provide proof of identity including full name and postal address
- An administration fee of £10 may be charged
- The response will be sent to the data subject by registered mail to a postal address within 40 days of receipt of the subject access.

Data Security

1. APR understands the need to keep personal data secure. In all cases personal data is stored electronically. One of the largest risks relating to data protection concerns the amount of personal data which is kept on laptops and computers .

2. APR will ensure that operating systems, firewall and anti-virus software on computers is up to date.

3. APR will ensure that personal computers can only be accessed using a password and are configured to automatically lock after a period of inactivity.

4. Personal data will not be held on mobile phone devices.