Data Protection and Confidentiality Policy

Rationale

EP Consulting is committed to a policy of protecting the rights and privacy of clients, staff and others, in accordance with the General Data Protection Regulation (GDPR) May 2018.

EP Consulting needs to process certain information about its staff, clients and other individuals with whom it has a relationship for various purposes to fulfil its duties.

To comply with various legal obligations, including the obligations imposed on it by the General Data Protection Regulation (GDPR), EP Consulting must ensure that all this information about individuals is collected and used fairly, stored safely and securely, and not disclosed to any third party unlawfully.

Compliance

This policy applies to all staff of EP Consulting. Any breach of this policy or of the Regulation itself will be considered an offence and the company's disciplinary procedures will be invoked.

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments to the GDPR and other relevant legislation.

General Data Protection Regulation (GDPR)

This piece of legislation came in to force on 25 May 2018. The GDPR regulates the processing of personal data, and protects the rights and privacy of all living individuals (including children), for example by giving all individuals who are the subject of personal data a general right of access to the personal data which relates to them. Individuals can exercise the right to gain access to their information by means of a 'subject access request'. Personal data is information relating to an individual and may be in hard or soft copy (paper/manual files; electronic records; photographs; CCTV images), and may include facts or opinions about a person.

The GDPR also sets out specific rights for staff in relation to personnel records held within the company's record system.

Responsibilities under the GDPR

EP Consulting will be the 'data controller' under the terms of the legislation - this means it is ultimately responsible for controlling the use and processing of the personal data.

The Directors are responsible for all day-to-day data protection matters, and will be responsible for ensuring that all members of staff and relevant individuals abide by this policy, and for developing and encouraging good information handling within the company.

Compliance with the legislation is the personal responsibility of all members of the company who process personal information.

Individuals who provide personal data to the company are responsible for ensuring that the information is accurate and up-to-date.

Data Protection Principles

In order to comply with its obligations, EP Consulting undertakes to adhere to the eight principles:

1. Process personal data fairly and lawfully.

2. Process the data for the specific and lawful purpose for which it collected that data and not further process the data in a manner incompatible with this purpose.

3. Ensure that the data is adequate, relevant and not excessive in relation to the purpose for which it is processed.

4. Keep personal data accurate and, where necessary, up to date.

5. Only keep personal data for as long as is necessary and dispose of any personal data in a way that protects the rights and privacy of the individual concerned (eg secure electronic deletion, shredding and disposal of hard copy files as confidential waste).

6. Process personal data in accordance with the rights of the data subject under the legislation.

7. Put appropriate technical and organisational measures in place against unauthorised or unlawful processing of personal data, and against accidental loss or destruction of data.

8. Ensure that no personal data is transferred to a country or a territory outside the European Economic Area (EEA) unless that country or territory ensures adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Subject Access Rights (SARs)

Individuals have a right to access any personal data relating to them which are held by the company. Any individual wishing to exercise this right should apply in writing to the Directors. Any member of staff receiving a SAR should forward this to the Directors.

Under the terms of the legislation, any such requests must be complied with within 40 days.

Disclosure of Data

Only disclosures which have been notified under the company's DP notification must be made and, therefore, staff should exercise caution when asked to disclose personal data held on another individual or third party.

EP Consulting undertakes not to disclose personal data to unauthorised third parties, including family members, friends, government bodies and in some circumstances, the police.

Legitimate disclosures may occur in the following instances:

- the individual has given their consent to the disclosure;
- the disclosure has been notified to a Director and is in the legitimate interests of the company;
- the disclosure is required for the performance of a contract.

Publication of Company Information

EP Consulting publishes various items which will include some personal data, eg:

- internal telephone directory.
- photos and information in social media / marketing materials.

It may be that in some circumstances an individual wishes their data processed for such reasons to be kept confidential, or restricted company access only. Therefore it is EP Consulting policy to offer an opportunity to opt-out of the publication of such when collecting the information.

Email

It is the policy of EP Consulting to ensure that senders and recipients of email are made aware that under the DPA, and Freedom of Information Legislation, the contents of email may have to be disclosed in response to a request for information. One means by which this will be communicated will be by a disclaimer on the company's email.

Under the Regulation of Investigatory Powers Act 2000, Lawful Business Practice Regulations, any email sent to or from the company may be accessed by someone other than the recipient for system management and security purposes.

CCTV

There is a CCTV system operating within EP Consulting for the purpose of protecting company's staff and property. EP Consulting will only process personal data obtained by the CCTV system in a manner which ensures compliance with the legislation.

Procedure for Review

This policy will be updated as necessary to reflect best practice or future amendments made to the General Data Protection Regulation (GDPR) May 2018 and Data Protection Act 1998.

For help or advice on any data protection or freedom of information issues, please do not hesitate to contact the Directors.

Last Reviewed: January 2019 By: Alan Latham, Director