Advance ITSM Ltd Data Protection Policy

It is Advance ITSM policy at all times to fully comply with current legislation and good practice in the capture, holding and subsequent disposal of data.

In this regard, consultants and associates engaged in work that may require the acquisition and use of customer data shall commit to:

- Ensuring that they comply with the six data protection principles, as summarised below
- Meeting their legal obligations as laid down by the General Data Protection Regulations (GDPR) 2018
- Ensuring that data is collected and used fairly and lawfully
- Processing personal data only in order to meet their operational needs or fulfil legal requirements
- Taking steps to ensure that personal data is up to date and accurate
- Establishing appropriate retention periods for personal data
- Ensuring that data subjects' rights can be appropriately exercised
- Providing adequate security measures to protect personal data
- Ensuring that a nominated officer is responsible for data protection compliance and provides a point of contact for all data protection issues
- Ensuring that all company officers are made aware of good practice in data protection
- Providing adequate training for all staff responsible for personal data
- Ensuring that everyone handling personal data knows where to find further guidance
- Ensuring that queries about data protection, internal and external to the organisation, are dealt with effectively and promptly
- Regularly reviewing data protection procedures and guidelines within the company

Data Protection Principles

1. Lawful, fair and transparent

There has to be legitimate grounds for collecting the data and it must not have a negative effect on the person or be used in a way they wouldn't expect.

2. Limited for its purpose

Data should be collected for specified and explicit purposes and not used in a way someone wouldn't expect.

3. Adequate and necessary

It must be clear why the data is being collected and what will be done with it. Unnecessary data or information without any purpose should not be collected.

4. Accurate

Reasonable steps must be taken to keep the information up to date and to change it if it is inaccurate.

5. Not kept longer than needed

Data should not be kept for longer than is needed, and it must be properly destroyed or deleted when it is no longer used or goes out of date.

6. Integrity and confidentiality

Data should be processed in a way that ensures appropriate security, including protection against unauthorised or unlawful processing, loss, damage or destruction, and kept safe and secure

Where appropriate, Advance ITSM will comply with agreed customer security policies.

To support this policy, the directors of Advance ITSM Ltd will take specific responsibility for Data Protection as Data Controllers.

All staff and associates will agree to the random checks of devices capable of storing, processing and transmitting data. Where staff have routinely or deliberately failed to comply with this policy, disciplinary action will be taken.

Any breach of regulation must be reported to the Directors and to the Information Commissioner within 72 hours.

May 2018

Ref.
Advance ITSM Data protection Process V A1.0
Data Protection Act (DPA) 1998
The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679)
General Data Protection Regulation (GDPR) May 25 2018