THE DATA CREW

ISMS DATA PROTECTION POLICY

ISO 27001 ISMS Polices & Procedures

Abstract

Sets out The Data Crew's rules on data protection and the legal conditions that must be satisfied.

THE DATA CREW

Didsbury Business Centre
137 Barlow Moor Road
Didsbury
Manchester
M20 2PW

ISMS Data Protection Policy

Policy Overview

This policy is based on ISO 27001:2013 the recognised international standard for information security. This standard ensures that the organisation complies with the following security principles:

- **Confidentiality**: all sensitive information will be protected from unauthorised access or disclosure;
- **Integrity**: all information will be protected from accidental, malicious and fraudulent alteration or destruction; and,
- **Availability**: Information services will be available throughout the times agreed with the users and be protected against accidental or malicious damage or denial of service.

The Data Crew is committed to ensuring that all these aspects of information security are complied with to fulfil its statutory functions.

Compliance with The Data Crew security policies and procedures is mandatory for all personnel.

The Chief Information Security Officer (CISO) approves this policy. The Information Security Forum (ISF) has the responsibility for ensuring that the policy is implemented and adhered to.

The security policy confirms The Data Crew commitment to continuous improvement and highlights the key areas to effectively secure its information.

Policy Scope

This part of our handbook sets out our rules on data protection and the legal conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transportation and destruction of personal information.

The Data Protection Officer is responsible for ensuring compliance with the General Data Protection Regulation (Regulation (EU) 2016/679). and with this part of our handbook.

If you consider that our provisions for complying with the General Data Protection Regulation have not been followed in respect of personal data about yourself or others you should raise the matter with your line manager.

Policy Detail

Definition of Data Protection Terms

Data is information which is stored electronically, on a computer, or in certain paper-based filing systems.

Data subjects for the purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.

Personal data means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal).

Data controllers are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They have a responsibility to establish practices and policies in line with the Act. We are the data controller of all personal data used in our business.

Data users include all staff of the Employer, irrespective of seniority, tenure and working hours, including all employees, directors and officers, consultants and contractors, casual or agency staff, trainees, homeworkers and fixed-term staff and any volunteers (Staff). whose work involves using personal data. Data users have a duty to protect the information they handle by following our data protection and security policies at all times.

Data processors include any person who processes personal data on behalf of a data controller. Employees of data controllers are excluded from this definition, but it could include suppliers which handle personal data on our behalf.

Processing is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

Sensitive personal data includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions and will usually require the express consent of the person concerned.

Data Protection Principles

Anyone processing personal data must comply with the eight enforceable principles of good practice. These provide that personal data must be:

- Processed fairly and lawfully.
- Processed for limited purposes and in an appropriate way.
- Adequate, relevant and not excessive for the purpose.
- Accurate.

- Not kept longer than necessary for the purpose.
- Processed in line with data subjects' rights.
- Secure.
- Not transferred to people or organisations situated in countries without adequate protection.

Fair & Lawful Processing

The Act is intended not to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject. The data subject must be told who the data controller is (in this case The Data Crew the purpose for which the data is to be processed by us, and the identities of anyone to whom the data may be disclosed or transferred.

For personal data to be processed lawfully, certain conditions must be met. These may include, among other things, requirements that the data subject has consented to the processing, or that the processing is necessary for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, more than one condition must be met. In most cases the data subject's explicit consent to the processing of such data will be required.

Processing for Limited Purposes

Personal data may only be processed for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted by the Act. This means that personal data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the data subject must be informed of the new purpose before any processing occurs.

Adequate, Relevant and Non-excessive Processing

Personal data should only be collected to the extent that it is required for the specific purpose notified to the data subject. Any data which is not necessary for that purpose should not be collected in the first place.

Accurate Data

Personal data must be accurate and kept up to date. Information which is incorrect or misleading is not accurate and steps should therefore be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data should be destroyed.

Timely Processing

Personal data should not be kept longer than is necessary for the purpose. This means that data should be destroyed or erased from our systems when it is no longer required.

Processing in Line with Data Subject's Rights

Data must be processed in line with data subjects' rights. Data subjects have a right to:

- Request access to any data held about them by a data controller.
- Prevent the processing of their data for direct-marketing purposes.

- Ask to have inaccurate data amended.
- Prevent processing that is likely to cause damage or distress to themselves or anyone else.

Data Security

We must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. Data subjects may apply to the courts for compensation if they have suffered damage from such a loss.

The Act requires us to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third-party data processor if he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself.

Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

- Confidentiality means that only people who are authorised to use the data can access it.
- Integrity means that personal data should be accurate and suitable for the purpose for which it is processed.
- Availability means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on our central computer system instead of individual PCs.

Security Procedures Include

- Entry controls. Any stranger seen in entry-controlled areas should be reported.
- Secure lockable desks and cupboards. Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)
- Methods of disposal. Paper documents should be shredded. Floppy disks and CD-ROMs should be physically destroyed when they are no longer required.
- Equipment. Data users should ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.
- Any data protection breaches must be reported to the Data Protection Officer who will ensure the breach is logged and investigated.

Dealing with Subject Access Requests

A formal request from a data subject for information that we hold about them must be made in writing. A fee is payable by the data subject for provision of this information. Any member of staff who receives a written request should forward it to their line manager immediately.

Providing Information over the Telephone

Any member of staff dealing with telephone enquiries should be careful about disclosing any personal information held by us. They should:

- Check the caller's identity to make sure that information is only given to a person who is entitled to it.
- Suggest that the caller put their request in writing if they are not sure about the caller's identity and where their identity cannot be checked.

Refer to their line manager OR the Data Protection Officer (DPO) for assistance in difficult situations. No-one should be bullied into disclosing personal information.

Review

This document must be reviewed at least annually by its 'Document Owner'. The Document Owner must ensure the correct version number is applied to the document once the review has taken place.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment

Compliance

The document owner or a nominated proxy will conduct regular compliance reviews of this document using the following template to record evidence of the review, along with any corrective or preventative actions that have been agreed as a result of non-compliance occurrences.

Signed

TOBIAS RILEY
CEO AME FUTURES LIMITED (THE DATA CREW)

Version Control

Version	Date	Author	Reviewed By	Approved By	Summary of Change
1.0	01/06/2016	Toby Riley	ISF	CISO	Initial Version.
2.0	01/06/2018	Toby Riley	ISF	CISO	Updated to reference GDPR.