Data Protection Policy

Contents

1 Introduction

Everyone has right to know how their personal information is handled. During the course of our activities with you we will collect, store and process personal information you supply as a customer and we recognise the need to treat it in an appropriate and lawful manner.

The types of information that we may be required to store include but are not limited to Company Details, Addresses, Contact Names, Email Addresses, Billing information including payment methods and may include your end client's information. This information may be held on paper or on a computer or other media, is normally subject to legal safeguards in the UK. Those safeguards impose restrictions on how we may use that information.

This policy may be amended at any time. Any breach of this policy will be taken seriously.

2 Status of the policy

This policy sets out our rules on data protection and the conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transportation, destruction of personal information and the access rights of Data Subjects

The Data Protection Officer (DPO) is responsible for ensuring compliance with our legal obligations with regard to the use of personal information and with this policy. That post is currently held by:

Colin Hudson
DPO
0333 222 8333
chudson@mediahawk.co.uk

Any questions or concerns about the operation of this policy should be referred in the first instance to the Data Protection Officer.

3 Definition of data protection terms

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

3.2 **Data Subjects** for the purpose of this policy include all living individuals about whom we hold personal data. A data subject may a national or resident of any country. All data subjects have legal rights in relation to their personal data.

3.3 **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).

3.4 **Data Controllers** are the people who determine the purposes for which any personal data is processed. They have a responsibility to establish practices and policies in line with the various legal frameworks that may affect our business.

3.5 **Data Users** include employees, contractors and 3rd parties whose work involves using personal data. Data users have a duty to protect the information they handle by following this policy at all times.

3.6 **Data Processors** include any person who processes personal data on behalf of a data controller.

3.7 **Processing** is any activity that involves use of the data and includes obtaining it, or even destroying it. Processing also includes transferring personal data to third parties.

3.8 **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 information about convictions sentenced against that person. Sensitive personal data can only be processed under strict conditions and will usually require the express consent of the person concerned.

4 Data protection principles

We follow the principles that are set by UK legislation (Article 5 Principles Relating to Personal Data Processing under GDPR regulations 25th May 2018).

Anyone processing personal data must comply with these enforceable principles of good practice.

The principles provide that personal data must be:

Lawfulness, Fairness and Transparency	Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject
Purpose Limitation	Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
Data Minimisation	Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
Accuracy	Personal data shall be accurate and, where necessary, kept up to date
Storage Limitation	Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
Rights of Data Subjects	Personal data shall be processed in accordance with the rights of data subjects
Integrity and Confidentiality	Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures
Data Transfers outside of EAA	Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection
Accountability	The controller shall be responsible for, and be able to demonstrate compliance with the GDPR

4.1 Lawfulness, Fairness and Transparency

4.1.1 This policy is not intended to prevent the processing of personal data, but rather 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, the purpose for which the data is to be processed and the identities of anyone to whom the data may be disclosed or transferred.

4.1.2 For personal data to be processed lawfully, certain conditions have to 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.

4.2 Purpose Limitations

4.2.1 Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of personal data for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes shall not be considered incompatible with the original processing purposes. However, conditions in GDPR Article 89(1) (which sets out safeguards and derogations in relation to processing for such purposes) must be met.

4.3 Data Minimisation

4.3.1 Personal data must be adequate, relevant and limited to those which are necessary in relation to the purposes for which they are processed.

4.4 Accuracy

4.4.1 Personal data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

4.5 Storage Limitation

4.5.1 Personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be stored for longer periods insofar as the data will be processed solely for archiving purposes in the public interest, financial, regulatory, scientific and historical research purposes or statistical purposes in accordance with Article 89(1) and subject to implementation of.

4.6 Rights of Data Subjects

4.6.1 Personal data shall be processed in accordance with the rights of data subjects and include,

the right of access to a copy of the information comprised in their Personal Data;

the right to object to processing that is likely to cause or is causing damage or distress;

the right to prevent processing for direct marketing;

the right to object to decisions being taken by automated means;

the right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed; and

the right to claim compensation for damages caused by a breach of the Act.

4.7 Integrity and Confidentiality

4.7.1 Personal Data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and

against accidental loss, destruction or damage, using appropriate technical or organisational measures.
Data Subjects may apply to the courts for compensation if they feel they have suffered damage from such a loss.

4.7.2 We have 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 that Processor agrees to comply with those procedures and policies, or if the processor puts in place adequate measures itself.

4.7.3 Maintaining Data Security means guaranteeing the confidentiality, integrity and availability of the Personal Data.

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 systems instead of local individual PCs.

4.7.4 Security procedures include:

Entry controls – secure building entry controls and to challenge any stranger seen in entry-controlled areas

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. CD-ROMs should be physically destroyed or shredded when they are no longer required, memory sticks and the like should be re-formatted

Equipment - data users should ensure that individual monitors do not show confidential to passers-by and that they log off from their PC when not in use

4.8 Data Transfers Outside of EEA

4.8.1 Personal Data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of Data Subjects in relation to the processing of Personal Data.

4.9 Accountability

4.9.1 The controller shall be responsible for, and be able to demonstrate compliance with the General Data Protection Regulation 2018 (GDPR)

5 Subject Access Rights (SAR)

5.1. You have the right to request access to your personal data. This request must be made in writing and, once received, depending on a limited number of exemptions, the organisation is required to provide the following information

I. a description of the personal data, the purposes for which it is processed, and whether it will / has been given to any other organisation or person;

II. the source of the data, except where that would identify another individual

III. all the information that forms the Personal Data record

IV. where a decision is taken by automated means, the logic employed in coming to the decision.

V. whether any personal data is being processed;

Mediahawk will provide the information within 40 days of application.

If you wish to make a request to access your information, please contact our Client Services Team at clientservices@mediahawk.co.uk or 0333 222 8333