**Introduction**

***Purpose***

We are committed to being transparent about how we collect and uses the personal data of our workforce, and to meeting our data protection obligations. This policy sets out our commitment to data protection, and individual rights and obligations in relation to personal data.

This policy applies to the personal data of job applicants, employees, workers, contractors, volunteers, interns, apprentices and former employees, referred to as HR-related personal data. This policy does not apply to the personal data of clients or other personal data processed for business purposes.

We have appointed Vicki Davies, HR Manager as the person with responsibility for data protection compliance within the organisation. Questions about this policy, or requests for further information, should be directed to Vicki Davies at [hr@oculusfm.co.uk](mailto:hr@oculusfm.co.uk)

***Definitions***

**"Personal data"** is any information that relates to a living individual who can be identified from that information. Processing is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

**"Special categories of personal data"** means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.

**"Criminal records data"** means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

**Data protection principles**

We process HR-related personal data in accordance with the following data protection principles:

* We process personal data lawfully, fairly and in a transparent manner.
* We collect personal data only for specified, explicit and legitimate purposes.
* We process personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
* We keep accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
* We keep personal data only for the period necessary for processing.
* We adopt appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

We tell individuals the reasons for processing their personal data, how we use such data and the legal basis for processing in our privacy notices. We will not process personal data of individuals for other reasons. Where we rely on our legitimate interests as the basis for processing data, we will carry out an assessment to ensure that those interests are not overridden by the rights and freedoms of individuals.

Where we process special categories of personal data or criminal records data to perform obligations or to exercise rights in employment law, this is done in accordance with a policy on special categories of data and criminal records data.

We will update HR-related personal data promptly if an individual advises that his/her information has changed or is inaccurate.

Personal data gathered during employment is held in the individual's personnel file (in hard copy or electronic format, or both), and on HR systems. The periods for which we hold HR-related personal data are contained in its privacy notices to individuals.

We keep a record of our processing activities in respect of HR-related personal data in accordance with the requirements of the General Data Protection Regulation (GDPR).

***Individual rights***

As a data subject, individuals have a number of rights in relation to their personal data.

*Subject access requests*

Individuals have the right to make a subject access request. If an individual makes a subject access request, we will tell him/her:

* whether or not his/her data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual;
* to whom his/her data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers;
* for how long his/her personal data is stored (or how that period is decided);
* his/her rights to rectification or erasure of data, or to restrict or object to processing;
* his/her right to complain to the Information Commissioner if he/she thinks we has failed to comply with his/her data protection rights; and
* whether or not we carry out automated decision-making and the logic involved in any such decision-making.

We will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless he/she agrees otherwise.

If the individual wants additional copies, we will charge a fee, which will be based on the administrative cost to we of providing the additional copies.

To make a subject access request, the individual should send the request to hr@oculusfm.co.uk. In some cases, we may need to ask for proof of identification before the request can be processed. We will inform the individual if we need to verify his/her identity and the documents we require.

We will normally respond to a request within a period of one month from the date it is received. In some cases, such as where we process large amounts of the individual's data, we may respond within three months of the date the request is received. We will write to the individual within one month of receiving the original request to tell him/her if this is the case.

If a subject access request is manifestly unfounded or excessive, we are not obliged to comply with it. Alternatively, we can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which we have already responded. If an individual submits a request that is unfounded or excessive, we will notify him/her that this is the case and whether or not we will respond to it.

*Other rights*

Individuals have a number of other rights in relation to their personal data. They can require us to:

* rectify inaccurate data;
* stop processing or erase data that is no longer necessary for the purposes of processing;
* stop processing or erase data if the individual's interests override our legitimate grounds for processing data (where we rely on our legitimate interests as a reason for processing data;
* stop processing or erase data if processing is unlawful; and
* stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override our legitimate grounds for processing data.

To ask us to take any of these steps, the individual should send the request to [email address].

**Data security**

We take the security of HR-related personal data seriously. We have internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties.

Where we engage third parties to process personal data on our behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

**Impact assessments**

Where processing would result in a high risk to individual's rights and freedoms, we will carry out a data protection impact assessment to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.

**Data breaches**

If we discover that there has been a breach of HR-related personal data that poses a risk to the rights and freedoms of individuals, we will report it to the Information Commissioner within 72 hours of discovery. We will record all data breaches regardless of their effect.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, we will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures we have taken.

**International data transfers**

We will not transfer HR-related personal data to countries outside the EEA.

**Individual responsibilities**

You are responsible for helping us to keep your personal data up to date. You should let us know if data provided to us changes, for example if you move house or changes your bank details.

You may have access to the personal data of other employees and of our customers and clients in the course of your employment. Where this is the case, we rely on you to help us meet our data protection obligations.

If you have access to personal data as part of your job, you are required:

* to access only data that you have authority to access and only for authorised purposes;
* not to disclose data except to individuals (whether inside or outside the organisation) who have appropriate authorisation;
* to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
* not to remove personal data, or devices containing or that can be used to access personal data, from our premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device;
* not to store personal data on local drives or on personal devices that are used for work purposes; and
* to report data breaches of which you become aware to [name] immediately.

Further details about our security procedures can be found in our data security policy.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under our disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

**Training**

We will provide training to all individuals about their data protection responsibilities as part of the induction process.

Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.