



Data Protection and Access to Information Policy

Aim and Scope of Policy

This policy applies to the processing of personal data in manual and electronic records kept by Metaverse VR in connection with employees, associates and clients. MVR will comply with the requirements of the 2018 Data Protection Act and other rights under the General Data Protection Regulation (GDPR). The policy also covers our response to any data breach.

This policy applies to the personal data of job applicants, existing and former employees, apprentices, volunteers, placement students, workers and self-employed contractors. These are referred to in this policy as relevant individuals.

Definitions of Types of Data (for the purposes of this Policy)

Personal Data: Information that relates to an identifiable person who can be directly or indirectly identified from that information, for example, a person's name, identification number, location, online identifier.

Special categories of Personal Data: Data which relates to an individual's health, sex life, sexual orientation, race, ethnic origin, political opinion and religion. It also includes genetic and biometric data (where used for ID purposes).

Criminal Offence Data: Data which relates to an individual's criminal convictions and offences.

Data Processing: Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

We are committed to ensuring personal data, including special categories of personal data and criminal offence data (where appropriate) is processed in line with GDPR and domestic laws. Where 3rd parties process data on behalf of MVR, we will ensure they take such measures to maintain our commitment to protecting data. In line with current data protection legislation, we understand we are accountable for the processing, management and regulation, and storage and retention of all personal data held in the form of manual records and on computers.

Types of Data Records

Personal data is kept in personnel files or stored on our “BrightHR” system. We may hold the following types of data on you, as appropriate:

- Name, address, phone numbers – for you and your next of kin
- CV and other information gathered during your recruitment
- References from your former employers
- Security Clearance and Right to Work information
- National Insurance number and Tax Code
- Job title, job description and pay grade information
- Conduct issues such as letters of concern, disciplinary proceedings
- Holiday record
- Internal performance information
- Medical or health information
- Sickness absence records
- Terms and Conditions of Employment
- Training record

Data Protection Principles

Any “Personal Data” or sensitive information we hold on you is covered by this legislation, including emails. “Personal data” is information that relates to an identifiable person who can be directly or indirectly identified from that information, for example, a person’s name, identification number, location, online identifier.

All “Personal Data” obtained and held by MVR will:

- Be processed fairly, lawfully and in a transparent manner
- Be collected for specific, explicit, and legitimate purposes
- Be adequate, relevant and limited to what is necessary for the purposes of processing
- Be kept accurate and up to date. Every reasonable effort will be made to ensure any inaccurate data is rectified or erased without delay
- Not be kept for longer than is necessary for its given purpose

- Be processed in a manner that ensures appropriate security of personal data including protection against unauthorised or unlawful processing, accidental loss, destruction or damage by using appropriate technical or organisational measures
- Comply with the relevant Data Protection procedures for international transferring of personal data.

In addition, “Personal Data” will be processed in recognition of your data protection rights, as follows:

- the right to be informed
- the right of access
- the right for any inaccuracies to be corrected (rectification)
- the right to have information deleted (erasure)
- the right to restrict the processing of the data
- the right to portability
- the right to object to the inclusion of any information
- the right to regulate any automated decision-making and profiling of personal data

If you receive a subject access request from a client, supplier or other 3rd party, you should refer this immediately to your line manager.

If you are a user of personal or sensitive information, please ensure you are not breaching any data protection rules when you store or use information and when you write and send emails. This could include but is not limited to:

- Using data which has not been kept up to date
- Passing on or processing personal information about an individual without their consent
- Keeping personal information longer than necessary
- Sending personal information outside the country

If any breach of data protection rules is discovered such as the leaking or hacking of personal or sensitive data, this should be reported immediately to your line manager, and any immediate action should be taken to close down such leaks. Your line manager will ensure this is properly investigated and the appropriate reporting actions taken if necessary.

MVR will hold and process the data relating to you in the course of your employment for administration and management purposes only. All such data will be treated confidentially and you may request reasonable access to your own personal data if you need to. You can request access to the information held on you by MVR. All requests to gain access to your records should be made in writing.

Changes to Personal Information for Employment Purposes

It is important our records are correct, as inaccurate, or out of date information may affect your salary or cause difficulties in situations where contact is required for emergencies. Please notify your line manager immediately of all changes, such as:

- Name
- Home address
- Telephone number
- Bank account details
- Examinations passed/qualifications gained
- Emergency contact
- Driving licence penalties (if you are required to drive on Company business)
- Criminal charge, caution or conviction
- Conflict, or potential conflict of interest

Data Protection Procedure

We have taken the following steps to protect your personal data, which we hold or have access to:

- We have appointed our COO as our “Data Processing Officer” who has specific responsibilities for:
 - the processing and controlling of data

- reviewing and auditing our data protection systems and procedures
- overseeing the effectiveness and integrity of all the data which must be protected.
- Through the provision of this policy we have provided you with an overview of your data protection rights, how we use your personal data, and how we will protect it.
- This policy also provides an overview of the importance of protecting personal data, and relevant individuals will be provided with training on how to treat information confidentially.
- We carefully control where “personal data” comes from, how it is stored and who it is shared with.
- We carry out risk assessments to identify any vulnerabilities in handling and processing “personal data”, and will take measures to reduce the risk of mishandling to prevent data breaches.
- The procedure includes an assessment of the impact of both use and potential misuse of personal data in and by the organisation.
- We recognise the importance of seeking your consent for obtaining, recording, using, sharing, storing and retaining your personal data, and regularly review our procedures for doing so, including the audit trails needed and followed for all consent decisions.
- We understand consent must be freely given, specific, informed and unambiguous. MVR will seek consent on a specific and individual basis where appropriate. Full information will be given regarding the activities about which consent is sought. You have the absolute and unimpeded right to withdraw that consent at any time.
- MVR have the appropriate mechanisms in place for detecting, reporting and investigating suspected or actual “personal data” breaches, including security breaches. We are aware of our duty to report significant breaches which cause significant harm to the affected individual(s) to the Information Commissioner, and we are aware of the possible consequences.
- We are aware of the implications of international transfer of personal data.

Access to Data

You have a right to be informed if we process “personal data” relating to you and can access the data we hold about you. Requests for access to this data will be dealt with under the following summary guidelines:

- There is a “Subject Access Request Form” on our Sharepoint and you will need to complete and submit the request to your line manager.
- We will not charge you for the supply of data unless your request is manifestly unfounded, excessive or repetitive.
- We will respond to your request without delay. Access to data will be provided, subject to legally permitted exemptions, within 1 month. This may be extended by a further 2 months where requests are complex or numerous.

Please inform your line manager immediately if you believe data held about you is inaccurate, either as a result of a subject access request or otherwise. We will take immediate steps to rectify the information.

Data Disclosures

We may be required to disclose certain data or information we hold about you to a person or 3rd party. Examples of circumstances leading to such disclosures include:

- any employee benefits operated by a 3rd party
- reasonable adjustments are required to assist you at work (injury or disability)
- health data – to comply with our Health & Safety or Occupational Health obligations towards you
- Statutory Sick Pay purposes
- HR management and administration – to consider how your health may affect your ability to do your role
- Effective operation and application of our employee insurance policies or pension plans.

We assure you these kinds of disclosures will only be made when strictly necessary.

Data Security

Our procedures are designed to maintain the security of your data, when it is stored and transferred. In support of our data security provisions, you are requested to do the following:

- Ensure all files or written information of a confidential nature is stored in a secure manner and is only accessed by people with a need and a right to access them
- Ensure all files or written information of a confidential nature are not left where they can be read by unauthorised people
- Refrain from sending emails containing sensitive work related information to your, or anyone elses, personal email address
- Check regularly on the accuracy of data being entered into any systems
- Protect security passwords provided to access our systems and do not share them with others who should not have them
- Ensure that “personal data” is not left on screen or printers when not in use.

“Personal data” relating to employees should not be kept or transported on laptops, USB sticks or similar devices. Where personal data is recorded on any such device, please protect it by:

- Ensuring data is only recorded on such devices where absolutely necessary
- Create a folder to store the files needing extra protection and all files created or moved to this folder should be automatically encrypted
- Ensure laptops or USB drives are not left lying around where they can be stolen.

Failure to follow our rules on data security may lead to disciplinary action, up to and including dismissal with or without notice dependent on the severity of the failure.

Training

Please ensure you read and understand this policy as part of your induction and on-boarding. Your line manager will also impart basic information to you about confidentiality, data protection and the actions to take if you identify a potential data breach.

Records

MVR keeps records of its processing activities including the purpose for the processing and retention periods. These records will be kept up to date so that they reflect current processing activities.

Data Processing Officer

The MVR Data Processing Officer is the COO.

©Metaverse VR Limited

Registered in England: 13684068, VAT No: GB 399750824.

Registered office: 3.05, Innovation and Collaboration Hub Portsdown Technology Park, North Hill Portsmouth, PO6 3RU

Tel: +44 (0) 2393 552 794 Email: info@metaverse-vr.co.uk