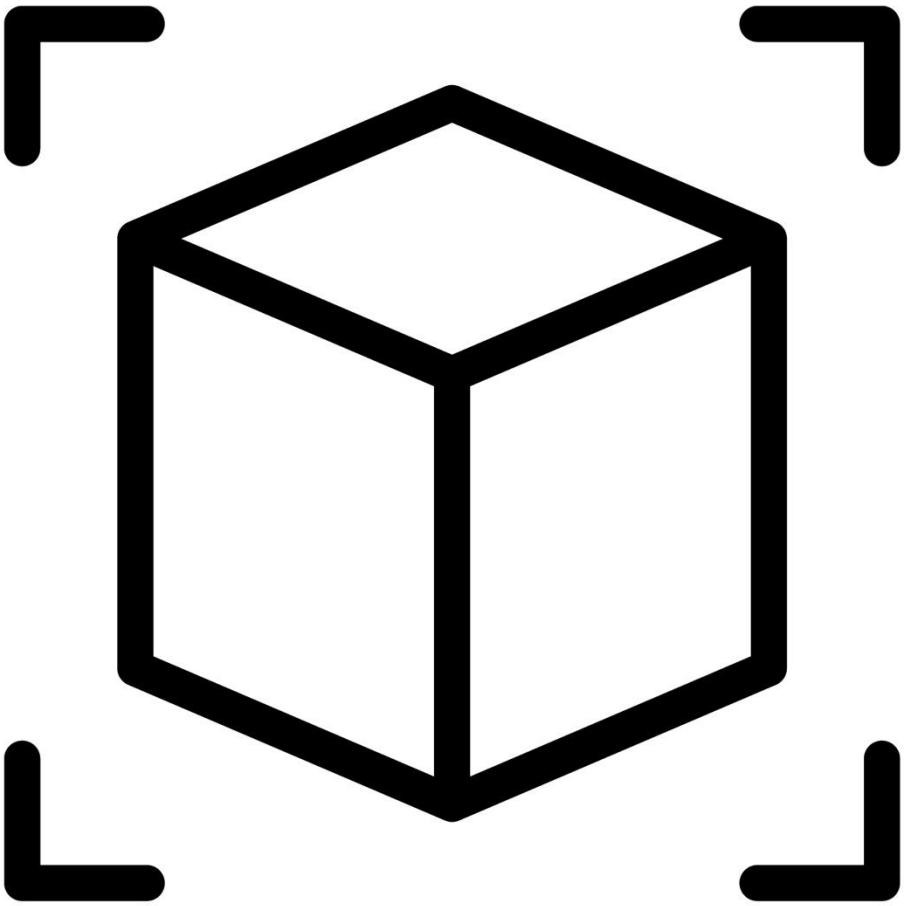
MRS Best Practice Guide on data collection activities in the metaverse

August 2024



Introduction

MRS has produced this Best Practice Guide to help practitioners act legally and ethically in collecting data in the metaverse.

Scope

Practitioners are required to give priority to local guidance i.e., where research practice takes place. This guidance is focusing on the collection of data from the UK, although the general principles and examples could apply and/or be adapted for other countries.

Context

This Guidance Note should be used in conjunction with the MRS Code of Conduct (2023) and MRS Guidance

MRS members and MRS Company Partners may contact the MRS Codeline Advisory Service with any specific queries.

Practitioners can use this guidance to assess whether they are complying with the MRS Code of Conduct in collecting data in the metaverse. This Guidance Note should be used in conjunction with the MRS Code of Conduct and Guidelines.

Interpretation of Requirements

When requirements use the word "must" these are mandatory requirements and is a principle or practice that applies the MRS Code of Conduct, which Members and Company Partners are obliged to follow.

The requirements which use the phrase "should" describe implementation and denotes a recommended practice. "May" or "can" refer to the ability to do something, the possibility of something, as well as granting permission.

Explanation of Key Terms

Definitions of the metaverse may vary and may include non-virtual reality environments, such as some online game platforms. For the purpose of this guidance the following definitions apply:

- ***Avatar*** is the representation of an individual in the metaverse. These representations can range from a motion picture like design to hyper realistic design.
- ***Augmented Reality (AR)*** are technologies that overlay virtual content on the real world so users can interact with digital content within this framework.
- ***Immersive technologies*** are a set of technologies that allow users to experience virtual environments in a more embodied way and reflect new ways of creating and interacting with digital applications and content.
- ***Metaverse*** – the metaverse is a virtual reality network in which anyone can join and collaborate with others. Users engage with a headset that immerses their sight and sound into virtual reality. They can do a wide range of activities, from playing games to talking in chat spaces to building worlds. Every user has a customizable avatar that can be a realistic or unrealistic representation of their identity.
- ***Virtual Reality (VR)*** are technologies that completely immerse a user in a virtual environment they can interact with, typically using head-mounted displays (HMDs).

Legal and Regulatory Obligations

The principles of the MRS Code of Conduct (2023):

MRS Members shall:

1. Ensure that their professional activities can be understood in a transparent manner.
2. Be straightforward and honest in all professional and business relationships.
3. Be transparent as to the subject and purpose of data collection.
4. Ensure that their professional activities are not used to unfairly influence views and opinions of participants.
5. Respect the confidentiality of information collected in their professional activities.
6. Respect the rights and well-being of all individuals.
7. Ensure that individuals are not harmed or adversely affected by their professional activities.
8. Balance the needs of individuals, clients, and their professional activities.
9. Exercise independent professional judgement in the design, conduct and reporting of their professional activities.
10. Ensure that their professional activities are conducted by persons with appropriate training, qualifications and experience.
11. Protect the reputation and integrity of the profession.
12. Take responsibility for promoting and reinforcing the principles and rules of the MRS Code of Conduct.

The Data Protection Act 2018 and the UK GDPR requires a legal basis for processing of personal data. Some personal data is categorised as 'special category data' and is subject to additional requirements when being collected.

Personal data categorised as special category data is data on:

- religious or philosophical beliefs
- health
- racial or ethnic origin
- trade union membership

- political beliefs
- sex life or sexual orientation
- genetic data
- biometric data (including photos when used for the purpose of uniquely identifying a natural person) of data subjects

The UK GDPR sets out seven key principles. These principles should lie at the heart of your approach to processing personal data:

- Lawfulness, fairness and transparency.
- Purpose limitation.
- Data minimisation.
- Accuracy.
- Storage limitation.
- Integrity and confidentiality (security)
- Accountability.

What are the lawful bases for processing?

The lawful bases for processing are set out in Article 6 of the UK GDPR. At least one of these must apply whenever you process personal data:

a. **Consent**: the individual has given clear consent for you to process their personal data for a specific purpose.

b. **Contract**: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

c. **Legal obligation**: the processing is necessary for you to comply with the law (not including contractual obligations).

d. **Vital interests**: the processing is necessary to protect someone's life.

e. **Public task**: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

f. **Legitimate interests**: the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

Ethical Design Considerations

1. Practitioner must inform participants at recruitment when metaverse and associated technologies (avatars, virtual or augmented reality environments) are being used.
2. Practitioners must take reasonable precautions to ensure that participants are not harmed or adversely affected by taking part in a data collection activity and ensure that there are measures in place to guard against potential harm. If participants are using avatars in a virtual or augmented reality environment, and are anonymous to each other, there is the potential for inappropriate behaviour in the absence of normal social constraints associated with being identifiable. Practitioners must brief participants on the rules of acceptable behaviour prior to the data collection activity to minimise harm, including the potential consequences for the participant if these rules are not followed, such as their removal from the activity and/or withholding an incentive. See the MRS Essential Safeguards series for advice on dealing with discriminatory comments and bullying and harassment
3. Practitioners must take reasonable steps to assess, identify and consider the particular needs of vulnerable people involved in their professional activities. Virtual or augmented reality environments may be unsettling for some participants and additional care must be taken when considering whether to involve vulnerable individuals in data collection activities in the metaverse. See the MRS Best Practice Guide on Research Participant Vulnerability
4. Practitioners must ensure that participants are not misled when being asked to participate in a project. Practitioners should be aware that whilst some participants will possess the skill sets and experience to fully engage in a data collection activity in the metaverse, others may be unfamiliar with the technology. Participants must be fully informed about the nature of any metaverse project and any requirements to allow participation, such as possessing any special skill set or wearable immersive technology equipment.
5. Practitioners must exercise special care when the nature of a project is sensitive. Consideration must be given to the subject matter of the data collection activity, and whether the subject matter is appropriate for discussion in a virtual or augmented reality environment. For sensitive topics, it may be more difficult for practitioners to display understanding and empathy, and due to the potential lack of non-verbal cues from participants avatars, it may be difficult to pick up on signs of distress or discomfort.
6. Practitioners must ensure that a participant's right to withdraw from a project at any stage is respected. Due to the potential lack of non-verbal cues from participants avatars, it may be difficult to pick up on signs of distress or discomfort or need to take a break from the data collection or withdraw completely. Practitioners must ensure that

there are withdraw mechanisms included within any metaverse projects.

7. Practitioners must ensure that the anonymity of participants is preserved unless participants have given their informed consent for their details to be revealed or for attributable comments to be passed on. Immersive technology wearables can collect a surge of data which could lead to the unintentional identification of participants. For some metaverse environments the default display name for participants is their full name. Participants must be made aware of this and encouraged to not use full names.

Data Protection Considerations
Special Category Data

1. Practitioners must always ensure that processing is generally lawful, fair and transparent and complies with all the other principles and requirements of the relevant national and international legislation relevant to a given project e.g., the UK data protection legislation. To ensure that processing is lawful, practitioners need to identify an Article 6 basis for processing.
2. Practitioners must consider the purposes of processing data for any metaverse project and identify which of these conditions are relevant for the data processing.
3. Practitioners must identify whether they need an 'appropriate policy document' (or similar) as required by data protection legislation, such as the UK's data protection legislation, when processing special category data. The Information Commissioner's Office (ICO) template appropriate policy document shows the kind of information this should contain.
4. Practitioners must complete a Data Protection Impact Assessment (DPIA) for any type of processing that is likely to be high risk. The nature of data processing using the metaverse means that it is more likely that projects will need a DPIA. For further information see the ICO guidance on DPIAs.
5. If practitioners process special category data when undertaking metaverse projects they must keep records, including documenting the categories of data. Practitioners may also need to consider how the risks associated with special category data affect their other obligations – in particular, obligations around data minimisation, security, transparency, Data Protection Officers (DPOs) and rights related to automated decision-making.

Additional Ethical Design Considerations

Data collection activities in the metaverse with children

1. The MRS Code of Conduct defines a child as an individual under the age of 16.
2. Practitioners must ensure that the environment in which the children have been invited to take part in the data collection is safe, and not at risk of encountering or engaging with strangers. Environments should be private, with appropriate measures in place to ensure the correct participants have joined the group. With the potential anonymity of visuals, audio and name, additional security such as a 2-factor verification system may need to be in place to ensure the identity and safety of child participants.
3. Practitioners must consider the age and level of understanding of any child participating in a data collection exercise in the metaverse.
4. Practitioners must give consideration about the data collection, security and safeguarding functionalities available when conducting data collection activities in the metaverse with children.

Examples of data collection activities in the metaverse

The following examples represent possible changes to how data collection activities may be conducted in the metaverse.

Virtual Focus Groups and Qualitative Research - Instead of meeting on a video conferencing platform, individuals could interact with their interviewees through the metaverse. This could make participants feel more comfortable, as they can maintain their anonymity while still feeling a person-to-person connection with the interviewer.

Product testing - A way of integrating data collection activities into the metaverse is through virtual product testing. This could mean having participants enter a virtual supermarket and monitoring which products they would purchase on an average shopping trip. Different simulations could include various iterations of the product design. Instead of asking participants what items they would choose to purchase, one could get a more realistic understanding of habits and brand perception by seeing how people act in a simulated setting.

Checklist

Practitioners should ask themselves and their clients the following questions when undertaking data collection activities in the Metaverse.

Design

- ☑ What type of data does the client want me to collect?
- ☑ Is the metaverse the most appropriate way to collect this data?

GDPR

- ☑ Is the data being collected via the metaverse relevant and not excessive?
- ☑ Is a Data Protection Impact Assessment (DPIA) and/or an ethics review required for this metaverse project?
- ☑ Has a DPIA and/or ethics review been completed and are there any changes and/or mitigations needed before the project starts?

Special category data

- ☑ Has the processing of the special category data been checked and is it necessary for the purpose/s identified?
- ☑ Has it been determined that there is no other reasonable and less intrusive way to achieve the purpose?
- ☑ Has an Article 6 lawful basis for processing the special category data been identified?
- ☑ Has an appropriate Article 9 condition for processing the special category data been identified?
- ☑ Where required, has an appropriate DPA 2018 Schedule 1 condition been identified?
- ☑ Have the special categories of data we are processing been documented?
- ☑ Is a DPIA necessary?

- ☑ Is there information about our processing of special category data in our privacy information supplied to participants?

- ☑ Have the risks associated with the use of special category data been considered including the other obligations around data minimisation, security, and appointing Data Protection Officers (DPOs) and representatives?

Data Collection

- ☑ What information needs to be gathered from the participants whilst using the metaverse?
- ☑ Is the data collection fit for purpose?
- ☑ Are participants able to express their views whilst using the metaverse? If not, what steps can be taken to ensure the data collection is fit for purpose?

Vulnerability

- ☑ Are the participants likely to be vulnerable?
- ☑ If participants are vulnerable have appropriate consents been gathered? Do these consents include sufficient information about the metaverse techniques being used?
- ☑ If there are vulnerable participants, has the MRS Best Practice Guide on Research Participant Vulnerability been referred to?

Useful Information Sources

MRS: MRS Code of Conduct 2019

MRS: Essential Safeguards – Dealing with discriminatory comments

MRS: Essential Safeguards - Bullying & Harassment

MRS: Best Practice Guide on Research Participant Vulnerability