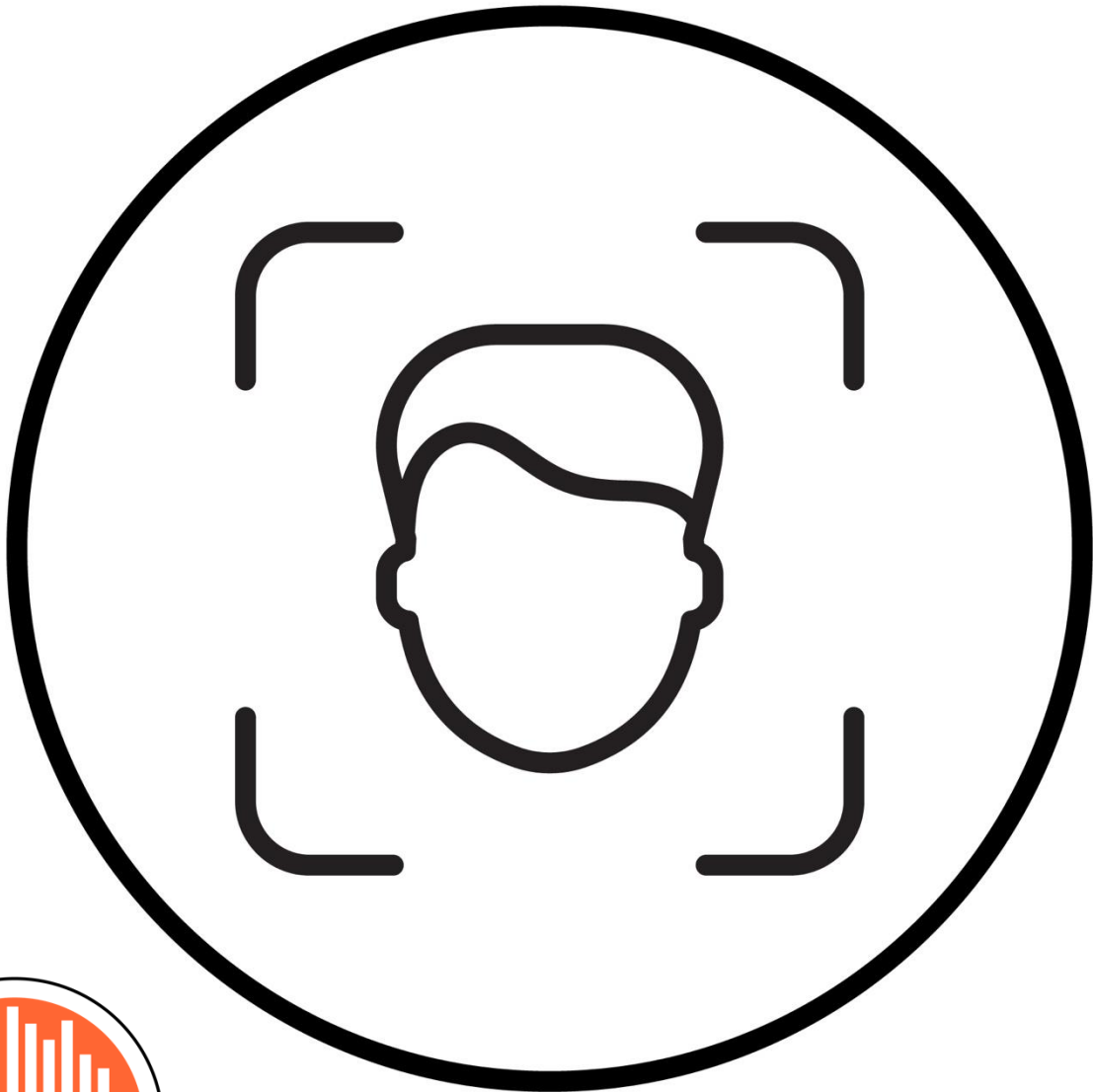




---

# Biometrics Data Guidance

June 2025



## Biometrics Data Guidance

### Introduction

MRS has produced this Best Practice Guide to help practitioners act legally and ethically in the collection and use of biometric data.

### 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.

This Guidance Note should be used in conjunction with the [MRS Code of Conduct \(2023\)](#) and other [MRS Guidance](#).

MRS members and MRS Company Partners may contact the [MRS Codeline Advisory Service](#) with any specific queries.

### Interpretation of Requirements

When requirements use the word “must” these are mandatory requirements and are 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.

### Context

Biometric data is a type of personal information. The General Data Protection Act (GDPR) defines biometric data as personal data resulting from specific technical processing relating to the physical, physiological, or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person.

Article 9 of the UK GDPR identifies certain types of personal information

as more sensitive and provides them with additional protection. These include biometric data when used for the purpose of uniquely identifying someone.

Not all biometric data is automatically special category biometric data. It only becomes special category biometric data if used to uniquely identify someone

Biometrics uses a variety of different technologies that mobilise probabilistic matching to recognise a person based on their biometric characteristics. Examples of biometric characteristics can be physiological features (such as, a person's fingerprint, iris, or hand geometry), or behavioural attributes (such as a person's gait or keystroke pattern).

As biometric characteristics are generally unique to individuals, they can be more effective and reliable at uniquely verifying the identity of individuals in comparison to other methods such as traditional verification systems (for example, a password or PIN).

Biometrics technologies in research, insight, data analysis and data collection can be considered both quantitative and qualitative and include observational and investigative research too. When practitioners gather biometric data, it is often numerical, this may include heart rate, eye-tracking patterns, or skin conductance levels. This numerical data can be analysed using statistical methods and provide quantitative measures of participants' physiological responses.

Alternatively, biometrics can provide qualitative insights into participants' emotions and attitudes. For example, researchers can use biometrics to measure changes in physiological responses, for example, as a participant views different products, or brand messages. These changes in physiological responses can indicate how participants feel and respond to the content they are viewing.

## Explanation of Key Terms

Types of biometric technology currently used in research, insight, data analytics and collection include:

**Biometric Data** means personal data resulting from specific technical processing relating to the physical, physiological, or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.

**Electroencephalography (EEG) technology** uses electrodes placed on the scalp to measure brain activity, providing insights into consumer engagement and attention levels.

**Eye-tracking technology** uses cameras and software to track eye movements and gaze patterns, providing insights into where participants are looking and focusing.

**Facial Recognition Technology** uses cameras and software to analyse facial expressions and emotions, such as smile intensity and eye movements.

**Galvanic Skin Response (GSR) technology** measures changes in skin conductance, which is related to the activity of sweat glands and is used as a measure of emotional arousal.

**Heart rate variability (HRV) technology** measures changes in heart rate and assesses emotional states such as excitement, stress, and anxiety.

## Relevant Definitions from the MRS Code of Conduct (2023)

**Client:** A client includes any individual, organisation, department or division, including any belonging to the same organisation as an MRS Member, which is responsible for commissioning or applying the results from a project.

**Data collection process:** a data collection process is any process used to obtain information from or about participants. It includes, but is not limited to, analytics tools, algorithms, interviews, as well as passive data collection.

**Natural person:** an individual that is an individual human being as opposed to other categories of person, for example legal definitions of legal persons.

**Participant:** is any individual or organisation from or about whom data is collected.

**Practitioners:** includes all individuals within the data collection supply-chain e.g., researchers, moderators, interviewers, recruiters, mystery shoppers, contractors, freelancers, and temporary workers.

**Research:** is the collection, use, or analysis of information about individuals or organisations intended to establish facts, acquire knowledge or reach conclusions. It uses techniques of the applied social, behavioural and data sciences, statistical principles and theory, to generate insights and support decision-making by providers of goods and services, governments, non-profit organisations and the general public.

**Special category data:** is the processing reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union Membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

**Vulnerable people:** Vulnerable people means individuals whose permanent or temporary personal circumstances and/or characteristics mean that they are less able to protect or represent their interests (see [\*MRS Best Practice Guide on Research Participant Vulnerability\*](#)).

## 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 UK Data Protection Act (DPA) 2018 and the UK GDPR requires a legal bases for the processing of personal data. Some personal data is categorised as 'special category data' and is subject to additional requirements when collected.

Special category data is data defined as:

- personal data revealing racial or ethnic origin;
- personal data revealing political opinions;
- personal data revealing religious or philosophical beliefs;
- personal data revealing trade union membership;

- genetic data;
- biometric data (where used for identification purposes);
- data concerning health;
- data concerning a person's sex life; and
- data concerning a person's sexual orientation.

More guidance about the requirements when collecting special category data is detailed in the MRS guidance, [\*GDPR in Brief No.10 – Collection of Ethnic Data and Other Special Category Data.\*](#)

## Examples of Biometric Technologies Used in Data Collection Processes

### An example of biometrics in research:

#### a Galvanic Skin Response and Eye Tracking Project

- Sample is recruited and brought to a focus group facility or research setting.
- Participants are asked to don galvanic skin response sensors on one hand.
- Participants surf through a website. Participants may be sitting next to practitioners, who asks them questions, or they may be self-directed.
- Practitioners will observe how participants naturally navigate through their experience.
- Depending on the technology employed, participants may either have face sensors attached, or their responses and eye tracking is captured through digital recordings.
- The biometric results are combined with other data collection (for example survey data), analysed and reported.

### An example of biometrics in research:

#### Facial Coding (quantitative)

- Participants were recruited to watch several variations of an advert and equipped with multiple biometric devices (facial expression and eye-tracking, EEG methods could also be employed)
- The research team observed participants' real-time biometric expressions
- The research team followed up with in-depth qualitative interviews to understand the reasons behind specific responses.

## An example of biometrics in research:

### Facial Coding

- Facial Coding shows us the true emotional response on a second-by-second basis as a person reacts to visual (usually video) stimulus.
- A sample is recruited and brought to a focus group facility or research setting.
- A webcam is set up in a research facility and participants are asked to watch a video whilst the webcam captures their expressions.
- Participants are often self-directed through the exercise. Practitioners will observe how participants naturally navigate through their experience.
- The responses can be measured against emotional criteria, such as: engagement, happiness, surprise, and negativity.
- These responses are then codified using an algorithm. Practitioners will evaluate facial coding at scale through an online environment.
- Depending on the technology employed, participants may either have face sensors attached, or their responses and eye tracking is captured through digital recordings.
- The biometric results are combined with other data collection (for example survey data), analysed, and reported.

## Ethical and legal Requirements and Considerations

### Design

#### The Rules

1. Members must ensure that their professional activities conform to the national and international legislation relevant to a given project, including the UK data protection legislation. Members must ensure that they adhere to all relevant legal and ethical requirements when conducting their professional activities.

**Comment:** See the [Data Protection & Research: Guidance for MRS Members and Company Partners](#)

2. Members must take reasonable steps to design projects to the specification and/or quality standards agreed with clients.
3. Members must carry out a Data Protection Impact Assessment (DPIA) or risk assessments for specified types of processing prescribed by data and privacy legislation and for any other processing that is likely to result in a high risk to participants. Comment: See the [MRS Standards & Policy Team webinar – 'Data protection Impact Assessment \(DPIA\) and Data Breach Reporting'](#)
4. Practitioners must always ensure that processing of biometric data is generally lawful, fair and transparent and complies with all the other principles and requirements of the UK GDPR. To ensure that processing is lawful, practitioners need to identify an [Article 6](#) basis for processing biometric data.
5. Practitioners must consider the purposes of processing biometric data and identify which of the Article 6 conditions are relevant.
6. Practitioners must also identify whether they need an 'appropriate policy document' as per the DPA 2018. The Information Commissioner's Office (ICO) [template appropriate policy document](#) shows the kind of information this should contain.
7. Practitioners must take reasonable action to ensure that participants are not harmed or adversely affected by taking part in any biometric data collection and processing activity and ensure that there are measures in place to guard against potential harm.

8. Practitioners must undertake [Data Protection Impact Assessment](#) (DPIA) for any type of processing that is likely to be 'high risk'. The ICO has identified a number of types of activities that could result in high-risk processing. Any processing of biometrics is included within this list. Practitioner therefore must undertake a DPIA for any projects where biometric data is collected.

**Comment:** See MRS Standards & Policy Team webinar – 'Data Protection Impact Assessment (DPIA) and Data Breach Reporting'.

## Data Protection Considerations – Special Category Data

### The Rules

1. Members must take all reasonable precautions to ensure that participants are not harmed or adversely affected by their professional activities and ensure that there are measures in place to guard against potential harm.
2. Practitioners should consider what necessary provisions and precautions must be taken to limit collecting unnecessary data such as, subconscious or highly sensitive data, which is not relevant to the research purpose. These risks and steps for mitigation must be addressed within a DPIA and Privacy notices. In the case that such sensitive data is inadvertently collected, it should be immediately identified and destroyed
3. Biometric data is classified as special category data when used for the purpose of uniquely identifying someone, this is typically referred to as 'special category biometric data'. Not all biometric data is automatically special category biometric data. It only becomes this if it is used to uniquely identify someone. The purpose for processing biometric data is therefore important. It defines whether special category biometric data is being processed.
4. It is important to note that biometric data may still be considered another type of special category information. If for example, biometric data could be used to infer someone's racial or ethnic origin or consider it as health data – this qualifies as special category data.
5. When practitioners process special category data 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.
6. Practitioners should consider the suitability of environments being considered for projects. Some biometric technologies, such as facial recognition, can be impacted by lighting conditions, camera quality, and the position and orientation of participants' faces. Biometric sensors can be impacted by external factors, such as movement, sweating, and changes in skin conductance.

7. Biometric technologies, such as facial recognition algorithms, can demonstrate higher error rates for people with darker skin tones, such as for some ethnic groups. Practitioners must take the necessary steps to alleviate bias in their data collection activities. This can be achieved by a number of activities such as:
  - a. **Mobilising diverse data sets:** When developing or testing biometric algorithms, practitioners should use a diverse data set that includes participants from diverse racial and ethnic backgrounds to ensure any algorithms used accurately measure physiological responses across a wide range of populations.
  - b. **Validate results:** Practitioners should compare biometric data to other forms of data, such as self-reported data, to ensure any biases are identified and addressed.
  - c. **Transparency:** Practitioners should be honest and transparent about methods used and the results generated, and any likely limitations of data collection processes and/or technology used.
  - d. **Monitor and Update:** Practitioners should continuously monitor and update their biometric algorithms to ensure they alleviate or remove any forms of racial biases presented in the algorithms and accurately capture physiological responses across diverse populations. See below on processing Special Category Data.

## Children and Vulnerable Adults

### The Rules

1. Members must ensure that permission of a responsible adult is obtained and verified before a child participate in their professional activities.

**Comment:** See the [MRS Guidelines for Conducting Data Collection Activities with Children](#)

2. Where the permission of a responsible adult is required, Members must ensure that the responsible adult is given sufficient information about the project to enable them to make an informed decision.
3. Members must ensure that the identity of the responsible adult giving permission to approach a child to take part in their professional activities is recorded by name, and relationship or role.
4. Where it is known (or ought reasonably to be known) that participants may include children, Members must ensure participants are asked to confirm their age before any other personal information is requested. Further, if the age given is under 16, the child must be excluded from giving further personal information until the appropriate permission from a responsible adult has been obtained and verified.
5. Members must take special care when considering whether to involve children in projects. The project design must take into account their age and level of understanding.

**Comment:** Privacy notices and other information supplied for a project must be presented in a format that can be understood considering age and level of understanding of child participants.

6. In all cases, Members must ensure that children have the opportunity to decline to take part, even when responsible adult permission has been obtained. This remains the case if a project takes place in school.
7. Members must take reasonable steps to assess, identify and consider the particular needs of vulnerable people involved in their professional activities

**Comment:** See the [MRS Best Practice Guide on Research Participant Vulnerability](#)

8. When working with vulnerable people, Members must ensure that such individuals are capable of making informed decisions and are not unfairly pressured to cooperate with a request to participate and that they are given an opportunity to decline to take part.
9. Practitioners must take reasonable action to assess, identify and consider the needs of vulnerable people involved in their professional activities. The use of biometric technologies may be unsettling for some participants, and additional care should be taken when considering whether to involve vulnerable individuals in data collection activities which use biometric technologies.
10. Under the MRS Code of Conduct, children are defined as those aged under 16 years. There is no recommended minimum age for data collection activities among children, but it is expected that practitioners would involve very young children directly in biometric data collection activities only when it is necessary and appropriate to a particular project.
11. Practitioners must ensure that participants are not misled when being asked to participate in a project. Practitioners should be aware that whilst some participants may understand the purpose and approaches used by biometric technologies, others may be unfamiliar with the technologies, and it may represent to them misuse with regard to their privacy.

## Data Collection

### The Rules

1. Members must exercise special care when the nature of a project is sensitive or the circumstances under which the data is collected might cause a participant to become upset or disturbed.
2. Practitioners should take reasonable action to address participant behaviour when using biometric approaches. For example, participants may alter their behaviour or emotions in response to being monitored, leading to uncharacteristic responses or behaviour, and resulting in inaccurate data.
3. Participants must be fully informed about the nature of the project, and what is required for their participation and which biometric technologies will be used, and the reason for their use in any project.
4. Practitioners must exercise special care when the nature of a project is sensitive. Consideration should be given to the subject matter of the data collection activity, and whether the subject matter is appropriate and suitable for the use of biometric technologies. For sensitive topics, practitioners may require support before, during and after data collection.
5. 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 during projects which use unconscious responses, it may be difficult, or responses may be conflated with the research project responses, which can make it difficult to pick up on signs of distress or discomfort or need to take a break from the data collection or withdraw completely. Practitioners should consider break times throughout any data collection to ensure the continued consent and well-being of participants.

## Data Security

### The Rules

1. Members must take reasonable action to ensure that all records are held, transferred and processed securely in accordance with relevant data retention policies and or/contractual obligations.
2. 49. Members 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.
3. Comment: This includes digital, audio or visual footage or photographs of identifiable participants which is classed as personal data.
4. Practitioners must take reasonable action to ensure that all biometrics data is held, transferred, and processed securely in accordance with relevant data retention policies and/or contractual obligations. The use of biometric data is unique to each participant and could lead to the unintentional identification and potential harm of participants if accessed or used inappropriately.

## Reporting

### The Rules

1. Members must provide clients with sufficient information to enable clients to assess the validity of results of projects carried out on their behalf.
2. Members must ensure that data include sufficient technical information to enable reasonable assessment of the validity of results.
3. **Comment:** Sufficient technical information, in the context of reporting inclusive data, would include reporting sampling characteristics and parameters used when defining samples as representative of segments of the population, such as when reporting Nationally Representative ('Nat Rep') or City Representative ('City Rep') samples.
4. See the four MRS Best Practice Guides on Collecting Sample Data which cover collecting data on ethnicity, sexual orientation, sex and gender and physical disabilities and/or mental health conditions for more detail.
5. 60. Members must ensure that outputs and presentations clearly distinguish between facts, opinion, and interpretation.
6. Members must ensure that findings disseminated by them are clearly and adequately supported by the data.
7. Practitioners must allow clients to arrange checks on the quality of outputs produced by biometric technologies.
8. Practitioners must be able to demonstrate the validity of research insights, conclusions and recommendations generated using biometric technologies.
9. Practitioners must consider and include in their privacy notice, efforts made to minimise harm to research participants.

**Comment:** This is required because biometric research projects can have the potential to discriminate against protected characteristics or reveal subconscious and highly sensitive personal data without the person's consent.

10. Practitioners must ensure that reports include sufficient information to enable reasonable assessment of the validity of results. This should include the means used to test and validate the accuracy of the technical and technological arrangements (e.g., algorithms) and methodologies utilised throughout a research project.
11. Practitioners must provide clients with sufficient information to enable clients to assess the validity of results carried out on their behalf using biometric technologies.
12. Comment: See the [MRS Code of Conduct](#) for more details about reporting requirements.

## Checklist:

Practitioners should ask themselves and their clients the following questions when undertaking data collection activities using biometric technologies.

### Design

- What type of data does the client want to collect?
- Is the collection of biometric data necessary?

### GDPR

- Is the data being collected relevant and not excessive?
- Has a DPIA been completed and are there any changes and/or mitigations needed?

### Special category data

- Is the processing of the special category data necessary for the purpose identified and is there other reasonable and less intrusive way to achieve that purpose?
- Is there an Article 6 lawful basis for processing the special category data?
- Is there an appropriate Article 9 condition for processing the special category data?
- Where required, has an appropriate DPA 2018 Schedule 1 condition been identified?
- Have the special categories of data being processed been appropriately documented?
- Is there specific information about the processing of biometric data as a special category of data been included in the privacy information provided to participants?
- Have the risks associated with the use of special category data been assessed with other obligations e.g., data minimisation, security, and appointing Data Protection Officers (DPOs) and representatives?

### **Data collection tool / Question Design**

- What information do I need to gather from the participants?
- What information do I need to relay to participants about the biometric data collection?
- Is the information about biometric data collection understandable to participants?
- Is the environment suitable for the collection of biometric data?
- Has participant anonymity been protected?
- Will sensitive topics be covered during the data collection? If so, what measures have been put in place to ensure that participants are not harmed as a result?

### **Children and Vulnerability**

- Are children and/or vulnerable adults involved in the data collection? If so, have appropriate consent measures been put in place?
- If there are children, has the MRS Guidelines: Conducting data collection activities with children been referred to?
- 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 2023](#)
- [MRS Guidelines: Essential Safeguards – Dealing with discriminatory comments](#)
- [MRS Guidelines for Conducting Data Collection Activities with Children](#)
- MRS: [Best Practice Guide on Research Participant Vulnerability](#)
- Data Protection & Research: Guidance for MRS Members and Company Partners
- Office of the Victorian Information Commissioner biometrics guidance: <https://ovic.vic.gov.au/privacy/resources-for-organisations/biometrics-and-privacy-issues-and-challenges/#introduction>
- Information Commissioner’s Office (ICO) Biometrics: Insight: <https://ico.org.uk/media/4021972/biometrics-insight-report.pdf>
- ICO: Biometric Data Guidance: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/>
- European Data Protection Board – Biometrics guidance: [https://www.edpb.europa.eu/our-work-tools/our-documents/topic/biometrics\\_en](https://www.edpb.europa.eu/our-work-tools/our-documents/topic/biometrics_en)
- National Cyber Security Guidance: Device Security Guidance: <https://www.ncsc.gov.uk/collection/device-security-guidance/policies-and-settings/using-biometrics>