



# Research Policy & Standards Webinar

Stay up-to-date and  
within the rules

- 
- Debrah Harding, FAcSS, FRSA
  - Managing Director, MRS
  - [#TweetMRS](#)



**1**

---

Domestic developments

---

**Debrah Harding**  
Managing Director

**2**

---

International and  
European updates

---

**Debrah Harding**  
Managing Director

**3**

---

MRS Guidance

---

**Julie Corney**  
Standards & Compliance  
Manager

# Employment Rights Bill Update

---



- The Employment Rights Bill is making its way through the Parliamentary process
  - The Bill is currently at the final stage for considering amendments before Royal Assent
  - The deadline for amending the Bill has been extended due to the number of amendments to be discussed – Royal Assent is expected this month, November
  - MRS met again with the DBT at the end of October to express concerns regarding the proposals for zero-hour contracts (ZHC) and whether these will affect flexible worker contracts used for interviewers
  - The overall message is that the ZHC provisions are due to be clarified in the Secondary legislation that will be drafted once the Employment Rights Bill is finalised
  - MRS will be responding to the consultation for the secondary legislation and continue to make representations as to why research contracts are inappropriate for the proposed guaranteed hours proposals
  - Any changes to ZHC will be introduced in 2027
-

# Data (Use and Access) Act – recognized legitimate interest

---



- The new Data (Use & Access) Act (DUA Act) received Royal Assent on 19 June 2025 with the changes due to be phased in between June 2025 and June 2026
  - Over the autumn the ICO consulted on new draft guidance on **recognised legitimate interest** – a new lawful basis for processing data introduced by the DUA Act
  - Recognised legitimate interest is one of the lawful bases for handling personal information
  - It is separate from the legitimate interest lawful basis
  - It has five conditions containing pre-approved legitimate interest purposes that are in the public interest
  - For these purposes, controllers do not have to assess whether a person's rights, freedoms or interests outweigh the recognised legitimate interest
  - Controllers do not have to change lawful basis if they currently use legitimate interests for a purpose that is a recognised legitimate interest
-

# Data (Use and Access) Act – recognized legitimate interest

---



- Annex 1 of the UK GDPR lists the pre-approved purposes
  - They cover situations where controllers need to use personal information to:
    - Share it with another organisation that has requested it because they need it for a public task or official functions (the 'public task disclosure request condition')
    - Safeguard national security, protect public security or for defence reasons (the 'national security, public security and defence condition')
    - Respond to, or deal with, an emergency situation (the 'emergencies condition')
    - Prevent, detect or investigate crimes, including the apprehension and prosecution of offenders (the 'crime condition')
    - Protect the physical, mental or emotional well-being of people who need extra support to do this or protect them from harm or neglect (the 'safeguarding condition')
  - The aim of introducing the "recognised legitimate interest" lawful basis is to give controllers greater confidence processing personal information for one of the pre-approved purposes
-

# Data (Use and Access) Act – recognized legitimate interest



- Recognised legitimate interest and legitimate interests are two separate lawful bases
- It is a choice which basis to rely on, so long as the requirements are met
- Below is a summary of the differences (from the ICO's website):

	Recognised legitimate interest	Legitimate interests
Suitable for a wide variety of purposes	✗	✓
Requires you to assess the impact on people's rights, interests and freedoms	✗	✓
Requires you to assess necessity	✓	✓
Right to object applies	✓	✓
Suitable as a basis for automated decision-making	✗	✗

# Data (Use and Access) Act – recognized legitimate interest

---



- Using legitimate interests as a lawful basis is more flexible, as it is not limited to a specific set of conditions
  - The three-part Legitimate Interest test does not apply to the recognised legitimate interest as the recognised legitimate interest are likely to meet the three-part requirements of the text, i.e.:
    - the purpose
    - what's necessary to achieve that purpose
    - balance these against people's rights, interests and freedoms
  - Controllers can use recognised legitimate interest for handling different types of personal information depending on the circumstances (e.g., special category data)
  - It may also be suitable for sharing personal information with other organisations, if controllers meet the requirements
-

# Data (Use and Access) Act – recognized legitimate interest



- 
- The safeguarding condition is one recognised legitimate interest that is relevant to research
  - To use the safeguarding condition controllers must:
    - ensure the use of the personal information counts as safeguarding
    - be satisfied that the person to be safeguarded is either a child or an 'at risk' adult
    - demonstrate that the processing of personal information is necessary to safeguard that person
  - Safeguarding in this context means:
    - protecting a "vulnerable individual" from neglect or physical, mental or emotional harm  
or
    - protecting the physical, mental or emotional well-being of a "vulnerable individual"
  - Only one of these needs to apply for use of personal information to be necessary for safeguarding
-

# Data (Use and Access) Act – recognized legitimate interest



- 
- The safeguarding condition only applies where the person involved is a “vulnerable individual”
  - The UK GDPR defines a “vulnerable individual” as:
    - a child (i.e., someone aged under 18); or
    - an adult who is ‘at risk’
  - All children and young people under the age of 18 are regarded in this context as “vulnerable”
  - However, for adults it depends on whether they are ‘at risk’. A person is ‘at risk’ if there is reasonable cause to suspect they:
    - need care and support
    - are either experiencing or are at risk of neglect or physical, mental or emotional harm and
    - as a result of those needs, are unable to protect themselves against the neglect, harm or risk
-

# Data (Use and Access) Act – recognized legitimate interest

---



- Controllers do not need to have explicit confirmation that an adult meets the 'at risk' criteria, though in some cases this might be already determined
  - When deciding whether someone is 'at risk' or not, controllers should take an objective and reasonable view, given all the information available
  - In order to be accountable, controllers should document their assessment of how an adult meets the criteria to be 'at risk' of vulnerability, including any evidence that supports this decision
  - Once determined as safeguarding a "vulnerable individual", controllers must determine if using personal information is necessary to safeguard them
  - This does not mean it has to be absolutely essential to process personal information for safeguarding but controllers must ensure it is more than just useful
-

# ICO consultation – 'soft opt in'

---



- Section 114 of the DUA Act will add a new regulation 22(3A) into the Privacy and Electronic Communications Regulations 2003 (PECR)
  - This change means charities will be able to send electronic mail marketing about their charitable purposes without the recipient's consent, if they meet several requirements
  - This exception only applies to marketing about a charities' similar products or services.
  - It doesn't apply to promoting aims and ideals (e.g., campaigning or fundraising)
  - However, charities must give data subjects a clear chance to opt out, both when data is first collected and every email sent thereafter
  - This is known as the 'charitable purpose soft opt-in' which is expected to take effect in January 2026, and charities cannot use it until then
-

# ICO consultation – 'soft opt in'

---



- Steps that should be taken to prepare for the charitable purpose soft opt-in include:
    - Reviewing processes for managing people's direct marketing preferences
    - Updating privacy notices to inform people about how their personal information will be used
    - Consider how to explain the charitable purpose soft opt-in to data subjects when collecting contact details including why they are receiving marketing communications from charities
    - When it commences from January 2026, charities should keep separate lists of data subjects who have consented to receive electronic mail marketing and those who will be sent communications using the charitable purpose soft opt-in
    - If applicable, charities could also have a separate list for people who receive electronic mail marketing about similar products and services using the commercial soft opt-in
    - Train relevant members of staff about how to respond to queries and complaints from people about the electronic mail marketing being received
-

# ICO consultation - enforcement

---



- The ICO is consulting on new guidance about the process they follow when carrying out investigations and taking enforcement action
  - The draft guidance explains the process the ICO follows for any investigation, from opening the case and information gathering, through to reaching a decision on whether to use statutory enforcement powers
  - It also explains some of the other ways in which the ICO may resolve compliance issues and the limits on the ICO's powers
  - The draft guidance will replace the existing statutory guidance set out in the Regulatory Action Policy published in November 2018
  - The DUA Act includes provisions that amend and add to ICO's existing powers
  - This includes new powers to require individuals to answer questions and to require organisations to plan for an approved person to prepare a report about a specified matter
  - The draft guidance reflects the changes to the ICO's powers in the data protection legislation following the DUA Act, which have either come into force or are expected to come into force in the coming months
-



## ICO breaches – Capita

---

- ICO have issued a fine of £14m to Capita for failing to ensure the security of personal data related to a breach in 2023 that saw hackers steal millions of people's information
- The cyber attack took place in March 2023
- The personal information of 6.6 million people was stolen, from pension records and staff records to the details of customers of organisations Capita supports.
- For some people, this included sensitive information such as details of criminal records, financial data or special category data.
- The ICO's investigation found that Capita had failed to ensure the security of processing of personal data which left it at significant risk, as well as lacking the appropriate technical and organisational measures to effectively respond to the attack

### **Points to note:**

- ICO initially informed Capita of an intended fine of £45m which was reduced following Capita submitting representations and mitigating factors on the provisional decision
  - Mitigations included improvements made after the attack, support offered to affected individuals and engagement with other regulators and the National Cyber Security Centre (NCSC)
-



# ICO breaches – Capita

---

## Summary of the contraventions:

Failure to prevent privilege escalation and unauthorised lateral movement:

- Capita did not implement a tiering model for administrative accounts allowing the attacker to escalate privileges, move laterally across multiple domains and compromise systems
- These failings were flagged as a vulnerability on at least three separate occasions but were not remedied

Failure to respond appropriately to security alerts:

- A high priority security alert was raised within ten minutes of the breach, but Capita took 58 hours to respond appropriately, against a target response time of one hour
- Capita’s Security Operations Centre was understaffed, and in at least six months before the incident fell well below the target response times for responding to security alerts

Inadequate penetration testing and risk assessment:

- Systems processing of records were only subject to a penetration test upon being commissioned and were not subject to any subsequent penetration test
  - Findings from penetration tests were siloed within business units - risks identified that affected the wider network were not universally addressed
-



## ICO breaches – Capita

---

This case highlights key areas the ICO's expectations about cyber security and what proactive steps organisations should be undertaking to reduce security risks, such as:

- Following [NCSC guidance on preventing lateral movement](#) and ensuring that the 'principle of least privilege' is applied across the organisation
- Regularly monitoring for suspicious activity and responding to initial warnings and alerts in a timely manner
- Sharing the findings from penetration testing across the whole organisation so risks can be universally addressed
- Prioritising investment in key security controls to ensure that they are operating effectively
- Checking agreements and responsibilities between data controllers and data processors

The NCSC reported that in mid-October 2025 "highly significant" [cyber attacks rose by 50%](#) over the last year, with UK security services dealing with new significant attacks more than every other day

---



## EU Adequacy recognition

---

- The European Data Protection Board (EDPB) has published mostly positive opinions on the UK's draft GDPR adequacy decisions published in July 2025
  - The EDPB says that 'most of the changes introduced to the UK's data protection framework aim to clarify and facilitate compliance with the law'
  - However, the EDPB has recommended that the European Commission should seek further clarifications on some aspects of the draft decision
  - The examples the EDPB mentions include data transfers from the UK to third countries, and the changes to the Retained EU Law (Revocation and Reform) Act 2023, also known as REUL Act - in particular the removal of the principle of primacy of EU law and the removal of the direct application of the principles of EU law
  - The EDPB says that with regard to data transfers from the UK to third countries, the new DUA Act 2025 requires the level of protection of the third country to be not materially lower than the one provided by the UK law - however, this test does not refer to the risk of government access, the existence of redress for individuals and the need for an independent supervisory authority
  - The EDPB calls on the Commission to further assess and monitor the changes to the ICO's structure
  - The UK's adequacy decision will expire on 27 December 2025, unless extended by the proposed six years until December 2031
-



# **International Update**

**Debrah Harding**



# Brazil Adequacy recognition

---



- On 4 September, the European Commission launched the process towards the adoption of a data protection adequacy decision with Brazil declaring that it ensures an adequate level of data protection on a similar basis to that of the EU
  - Once adopted, this will be the first EU GDPR adequacy decision for Latin America since Argentina on 3 June 2003 and Uruguay on 21 August 2012
  - The adopted decision would allow for free and safe data flows for businesses, public authorities, and research projects between the EU and Brazil under the EU GDPR
  - The Brazilian authorities have also initiated a process to adopt an equivalent decision to allow for Brazilian data to flow freely to the EU
  - The next steps will be for the draft decision to be reviewed by the European Data Protection Board and the Council of Ministers representing the EU Member States
  - The European Parliament also has a right to scrutinise this draft adequacy decision
-



## EU Digital Simplification

---

- Over the autumn the EU Commission's undertook a consultation seeking views on simplification measures for the AI Act and the EU's ePrivacy legislation
  - MRS responded to this consultation via the European Research Federation, EFAMRO
  - The EU's ePrivacy legislation is outdated but attempts to modernise have so far failed
  - The Commission recognises cookie consent fatigue, and the need to strengthen users' digital rights online
  - Equally, the Commission aims to facilitate the use of cookies and other technologies for business
  - A further objective is ensuring the predictable application of the AI Act as implementation challenges have already been identified
  - The Commission has previously proposed certain simplifications to the GDPR's provisions on activities such as Records of Processing Activities, but has not expanded on this proposal
  - There remains some political pressure both within the EU and from other countries, particularly the US, about the EU's approach to digital regulation
-

# International data issues - TikTok

---



- In May 2025 the Irish Data Protection Commission issued a decision that TikTok infringed the GDPR regarding its transfers of EEA User Data to China and its transparency requirements
  - The DPC ruled that TikTok was in breach of GDPR because the Standard Contractual Clauses and supplementary measures it relied upon were insufficient to address the risks of access by public authorities under Chinese law
  - The DPC also found that TikTok Ireland violated the transparency obligations of the GDPR by failing to adequately inform users of the details and risks of the data transfer
  - The decision included administrative fines totalling €530 million and an order requiring TikTok to bring its processing into compliance within 6 months
  - The decision also included an order suspending TikTok's transfers to China if processing is not brought into compliance within this timeframe
-

# International data issues - TikTok

---



- **Points to Note:**

- The DPC's decision is based on a crucial legal interpretation: remote access to personal data by personnel in a third country itself constitutes a "transfer" as defined in Chapter V of the GDPR
  - Regardless of where data is stored globally outside of China, such as the EU, when an employee located in China views or processes that data, this action means the data is being processed on a computer information system within China
  - Therefore, this constitutes a cross-border transfer under the GDPR, and compliance obligations must be fulfilled
  - The physical location of data servers is no longer the determinative factor in the analysis of data transfers
  - The regulatory focus has irrevocably shifted to the location of the personnel who can access this data
  - The DPC decision indicates that if the issue of access permissions is not fundamentally resolved, technical and contractual measures cannot remedy the fundamental flaws in the cross-border data transfer framework
  - Standard Contractual Clauses bind the relevant corporate entities but have no legal effect on state authorities – such as China where the data could be subject to access requests from the Chinese government
-

# ECJ decision – anonymous data

---



- **Deloitte and Single Resolution Board**

- On 4 September 2025, the ECJ issued major decision on the scope of personal data, accepting the point that pseudonymised data may be anonymised in the hands of a third party
  - The background to the case was the sharing of a dataset by the Single Resolution Board (SRB) with Deloitte, which had been tasked by SRB with carrying out a valuation
  - SRB took a series of steps to protect the dataset shared with Deloitte, including applying pseudonymisation measures to the dataset
  - Deloitte had no access to the original database, and SRB retained a code which allowed it to reidentify the dataset
  - The dataset sent to Deloitte included an alphanumeric code but not the reidentification code
  - SRB did not include information in its privacy notice that Deloitte was a potential recipient of the personal data
  - Following this sharing, the European Data Protection Supervisor (EDPS) received five complaints from data subjects and found that the data was personal data (pseudonymised) because SRB retained the reidentification code
  - At the heart of the dispute was whether anonymisation should be an absolute or relative test
  - The EDPS adopted an absolute approach, and if the court had accepted EDPS's view, this would mean it would never be possible for data to be anonymous if any person retained the code
-



## ECJ decision – anonymous data

---

- **Points to note:**
  - The key legal question reviewed by the ECJ was whether the data relates to identified or identifiable persons
  - It was accepted that the persons were not identified, so the key point is whether the persons were identifiable
  - The court rejected the EDPS interpretation
  - Instead, the ECJ confirmed that, contrary to the opinion of the EDPS and EDPB, pseudonymised data may, depending on the circumstances of the case, ensure that persons are no longer identifiable
  - More importantly, the ECJ found that the fact that SRB held the reidentification code did not necessarily mean the data was personal data – there was a need to look whether Deloitte had legal means available to re-identify the data
  - The court did agree with EDPS in one area – SRB, as the controller had breached its transparency obligations because it did not tell data subjects that the data was being transmitted to Deloitte, regardless of whether such data was personal data from Deloitte’s perspective
  - The ECJ’s decision is consistent with the approach taken by the ICO
-

# International data issues – Disney

---



- Disney has agreed to pay a \$10 million civil penalty for allowing children’s data to be collected on videos posted to YouTube
  - The Federal Trade Commission alleged that Disney failed to designate videos on the platform as “Made for Kids” (MFK)
  - This designation is meant to comply with US federal law that protects children from having their data collected and used for targeted advertising
  - The FTC reported that Disney will change its practices to comply with the Children’s Online Privacy Protection Act, which requires parental consent for data collection for users under 13 years old
  - Disney has agreed to establish and implement a program to review whether videos posted to YouTube should be designated as MFK
  - **Points to note:**
  - Whilst the UK has the data protection and Online Safety Act requirements, there are other rules such as COPPA which must be followed
-

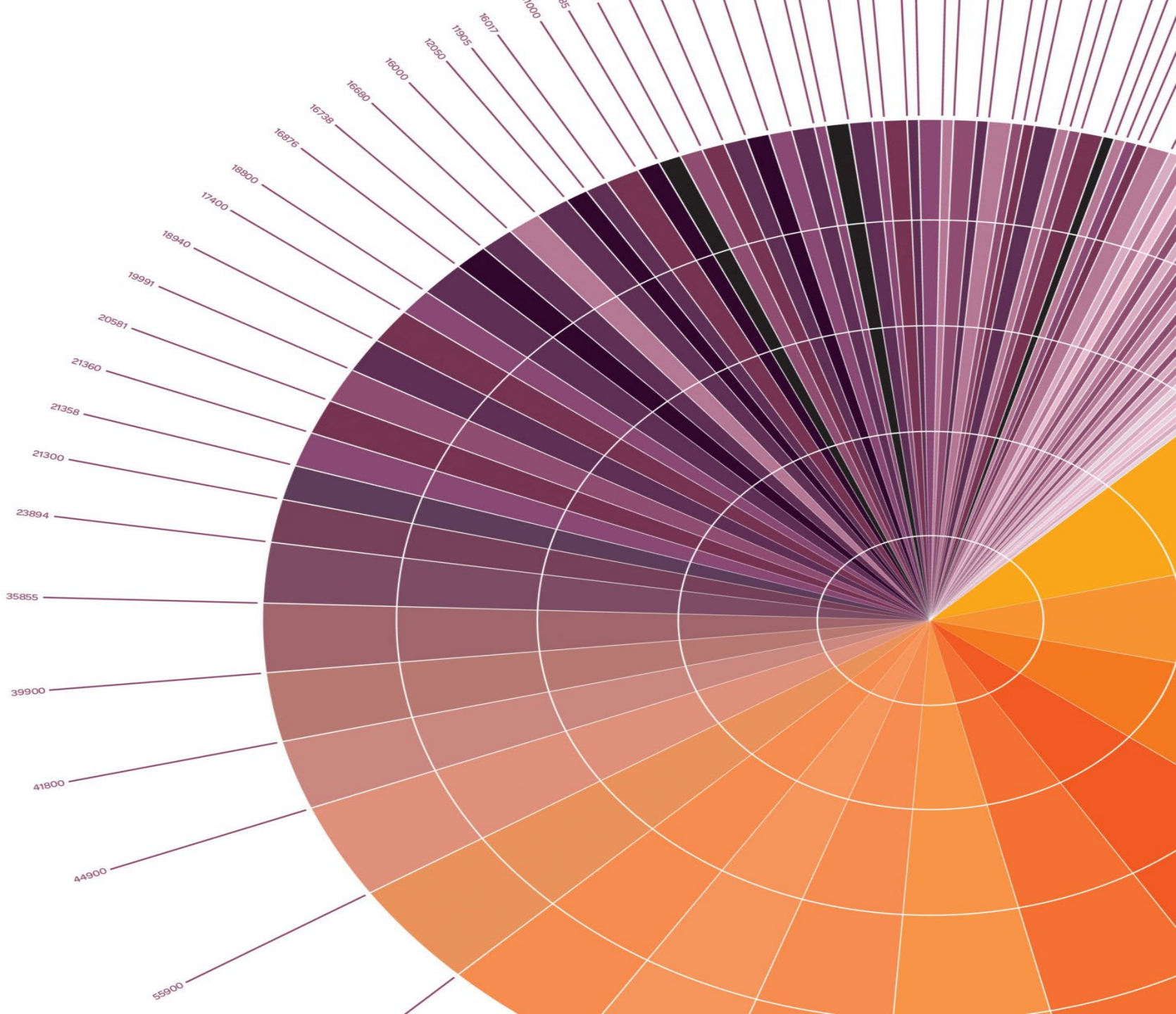


# **MRS Guidance update**

**Julie Corney**



# MRS Best Practice Guide on Accessible Data Collection Activities



# **MRS Best Practice Guide on Accessible Data Collection Activities**

---



The aim of this guidance is twofold:

- To provide an overview of the European Accessibility Act 2025 and its implications for practitioners; and
  - To bring together relevant, existing MRS guidance into one document as a useful reference of the legal and ethical issues to be considered when undertaking research with practitioners with accessibility considerations.
-

# **MRS Best Practice Guide on Accessible Data Collection Activities**

---



## **The European Accessibility Act (EAA) 2025**

The European Accessibility Act (EAA), which aims to improve the accessibility of products and services for people with disabilities within the EU, will come into force on June 28, 2025. The EAA applies to any organization that provides products and services to consumers in the EU, including businesses and public bodies in the UK. While the UK is not a member of the EU, it is still expected to comply with the EAA if it sells products or services to EU consumers.

---

# MRS Best Practice Guide on Accessible Data Collection Activities

---



## Key aspects of the EAA

- **Scope** – the EAA covers a wide range of products and services
  - **Compliance** – businesses must ensure they meet requirements
  - **Accessibility Standards** - harmonize accessibility requirements
  - **Impact on UK businesses** – ensure compliance to avoid risk
  - **Benefits for individuals** - persons with disabilities and elderly people should benefit
-

# MRS Best Practice Guide on Accessible Data Collection Activities

---



## Key aspects of the EAA

- **Enforcement and Penalties** – member state responsible
  - **Reporting non-compliance** – possible for consumers to report
  - **Products and service covered** - the EAA covers products and services that have been identified as being most important for persons with disabilities while being most likely to have diverging accessibility requirements across EU countries.
-

## **MRS Senior Client Council: Diversity & Inclusion Best Practice Guides**

---



This guidance provides a client perspective on inclusion and has been prepared by members of the MRS Senior Client Council and client colleagues.

The MRS Code of Conduct requires transparent information about which sampling characteristics and parameters have been used when defining samples as representative of segments of the population, such as when reporting Nationally Representative samples.

---

## **MRS Senior Client Council: Diversity & Inclusion Best Practice Guides**

---



### **Some examples include:**

#### **For Quantitative research:**

- Using visual stimuli and images to illustrate ideas or concepts
  - Using faces (rather than a number scale) can be more inclusive for those who English isn't first language, as well as those with specific learning difficulties
  - Ensure adequate contrast between text, background, and images
  - Do not use colour as the only means of conveying information
-

## **MRS Senior Client Council: Diversity & Inclusion Best Practice Guides**

---



### **For Qualitative research:**

- Consider any materials being shown (colour of text etc.)
  - Consider how you set up the room – and allow people to choose where they sit
  - Allow participants to complete tasks in their own time/at their own speed
  - Have the technology to support virtual groups, such as closed captioning
  - Allow participants extra time if needed
-

## Collecting Sample Data on Physical Disabilities and/or Mental Health Conditions

---



### Key points to consider:

- Provide adequate preamble/context before physical disabilities and/or mental health questions are asked
  - Be clear as to which category of physical disabilities and/or mental health condition data needs to be collected
  - Physical disabilities and/or mental health conditions questions should be placed together
  - Encourage clients to consider the level of detail required
  - Respect privacy of participants
-

# Collecting Sample Data on Physical Disabilities and/or Mental Health Conditions

---



## Key points to consider continued

- Balance data collection needs against the potential for intrusion
  - Privacy notice
  - Open responses
  - Provide additional guidance
-

## Essential Safeguards series: Conducting data activities with neurodiverse individuals

---



### Designing inclusive research sessions

When designing research practitioners should consider neurodiverse participant needs. For example:

- **Accessibility**
  - **Communication**
  - **Inclusivity**
-

## **Essential Safeguards series: Conducting data activities with neurodiverse individuals**

---

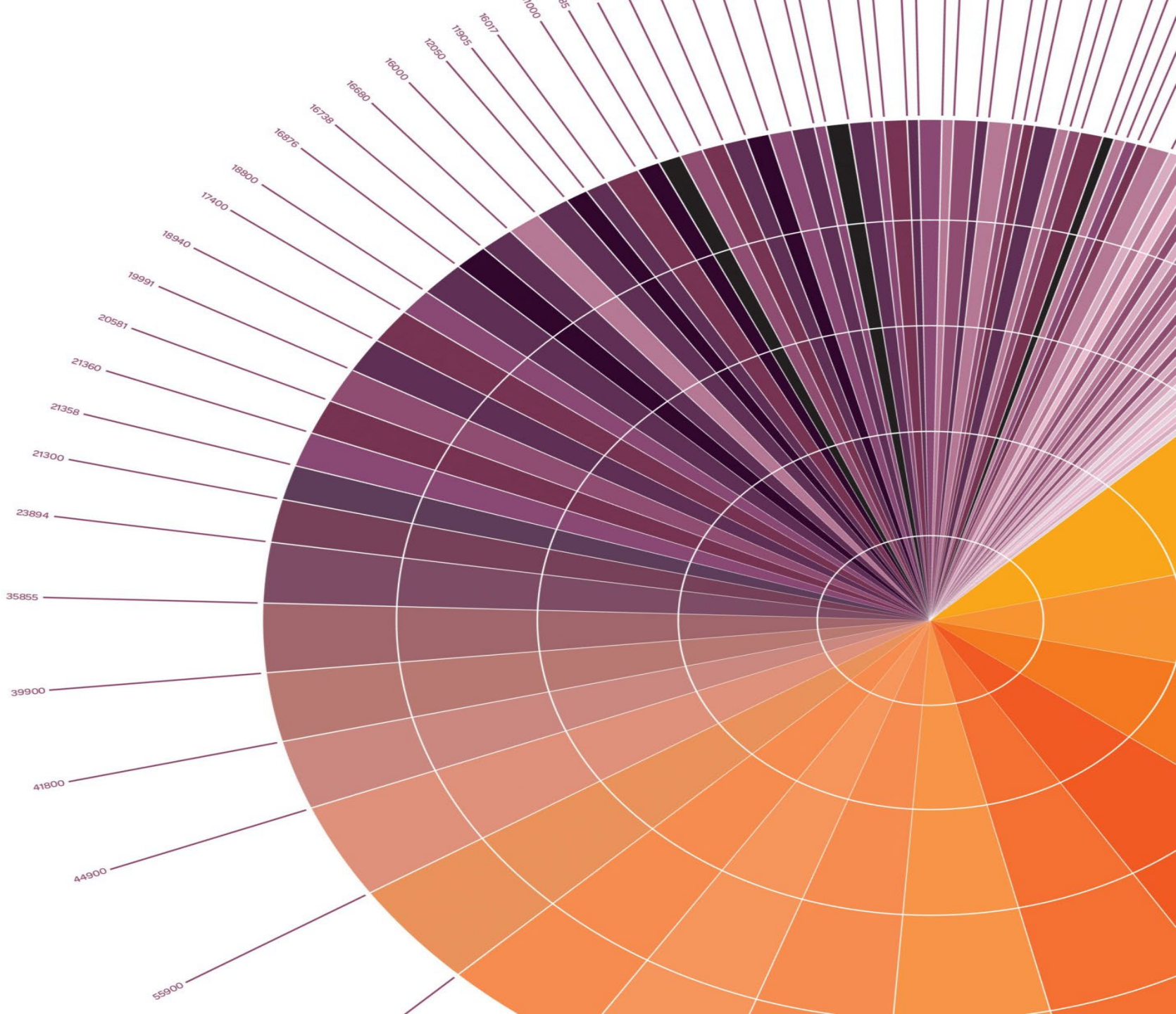


### **Designing inclusive research sessions continued**

Some further considerations:

- **Plan session stimulus**
  - **Remove participation barriers**
  - **Make participants feel comfortable**
-

# MRS guidance on how to read opinion polls





## **How to read opinion polls**

---

### **Opinion Polls – The Essential Points**

#### **What is an Opinion Poll?**

An opinion poll is a survey of public opinion obtained by questioning a representative sample of individuals selected from a clearly defined target audience or population. For example, it may be a survey of c. 1,000 UK (England, Scotland, Wales and Northern Ireland) adults aged 18 years and over. When conducted appropriately, opinion polls can add value to the national debate on topics of interest.

Typically, individuals or organisations commission a research organisation to undertake an opinion poll. The results to an opinion poll are either carried out for private use or for publication.

---



## How to read opinion polls

---

### Questions to Ask when Evaluating Opinion Polls

- Who has commissioned the opinion poll?
  - Who has undertaken the opinion poll research?
  - Has the opinion poll been carried out among the appropriate and clearly defined target audience / population? Are there any groups missing?
  - Is the methodological approach appropriate?
  - Is the sample representative of the target audience / population, or not?
-



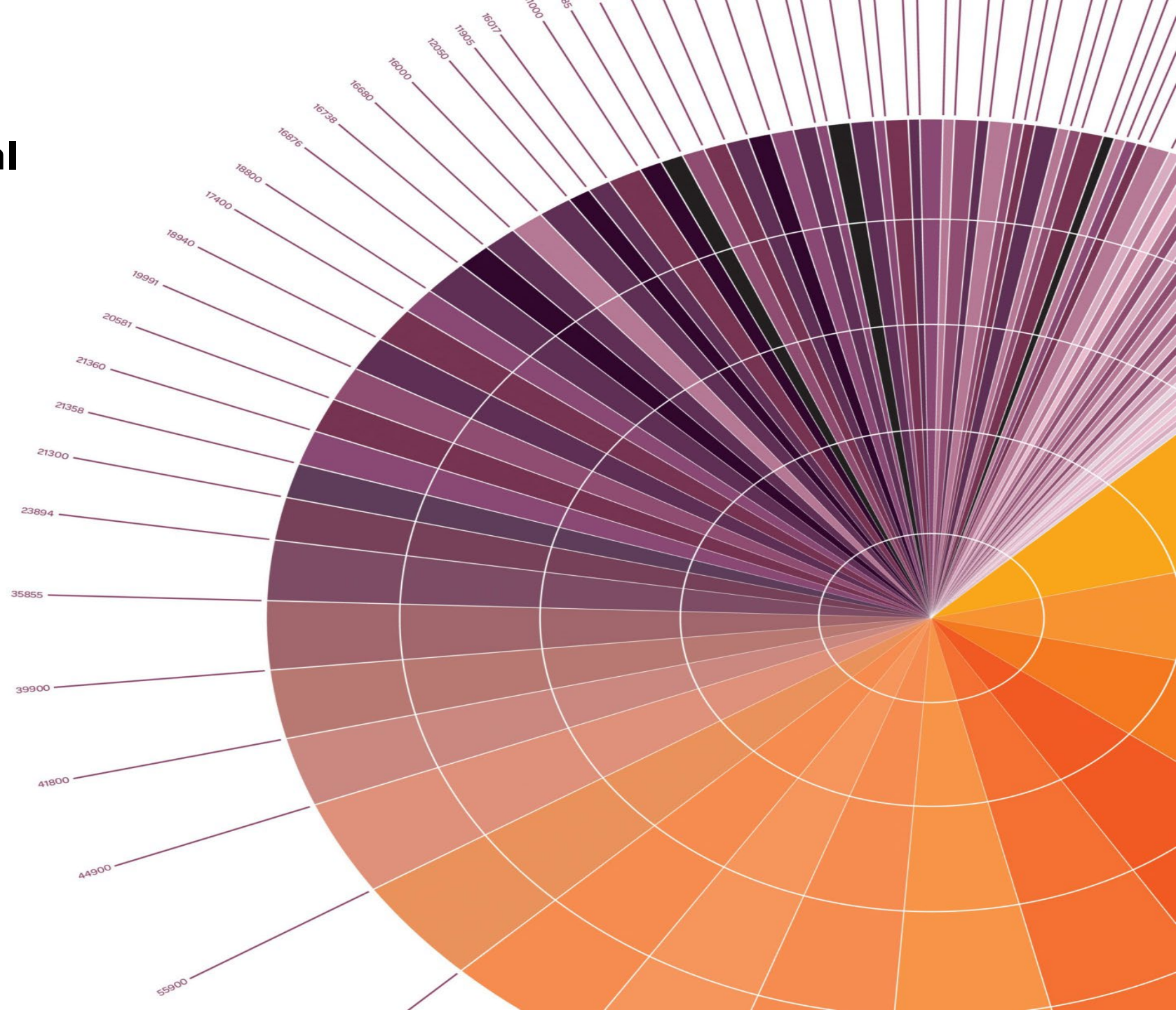
## How to read opinion polls

---

### Questions to Ask when Evaluating Opinion Polls continued

- Are the questions asked appropriate, accurate, balanced and unambiguous?
  - Have the survey data been weighted and is the weighting accurate?
  - Are the data tables / analysis accurate and, if published, is there a Technical Note accompanying the tables / analysis?
  - Is the commentary on the results accurate?
  - Full details of the Opinion Poll
-

# MRS Best Practice Guide on Collecting Data on Biological Sex and Gender Identity



# **MRS Best Practice Guide on Collecting Data on Biological Sex and Gender Identity**

---



MRS has produced this Best Practice Guide to help practitioners act legally and ethically in collecting data and asking research participants questions on biological sex and gender identity.

Providing universally accepted definitions of 'sex' and 'gender' is challenging, as these terms and their implications are not standardised. However, while recognising this and acknowledging the ongoing and evolving debate about language, for the purposes of this guidance, we have interpreted key terms as follows.

---

## MRS Best Practice Guide on Collecting Data on Biological Sex and Gender Identity

---



**Sex** refers to biological and physiological characteristics and to a person's physical anatomy. Sex is also recorded at birth based on biology and physiological characteristics, and that in the UK sex at birth is recorded in a binary way (male/female).

The Office for National Statistics (ONS) defines **gender identity** as a person's internal, personal sense of their own gender, which may not match the sex they were registered at birth. It is a person's sense of being male, female, or another identity such as non-binary. This personal perception differs from the legal/biological concept of sex, which is based on characteristics like chromosomes.

**Transgender** is a term generally used to describe people whose gender identity does not match their sex recorded at birth. Transgender people identify with a range of gender identities such as non-binary, transgender man, transgender woman or may identify as male or female.

---

# MRS Best Practice Guide on Collecting Data on Biological Sex and Gender Identity

---



Practitioners should ask themselves and their clients the following questions when undertaking projects which use, collect or report data on biological sex and gender identity:

## **Design**

- What type of data does the client want me to collect? Biological sex, gender identity or both? If the survey is to be weighted by sex, then this must be collected, and gender identity should not be used as a proxy.
  - If a project is using a representative sample e.g., Nat Rep or City Rep samples, does this sample approach include participants biological sex and gender identity?
  - Do I need to collect data on biological sex, gender identity, or both types of data need to be collected?
-

# **MRS Best Practice Guide on Collecting Data on Biological Sex and Gender Identity**

---



- Is there a research purpose for collecting data on biological sex, gender identity, or both?
- Is the data being collected relevant and not excessive?
- Is there a clear purpose for collecting biological sex and/or gender identity data?

## **Question Design**

- What information do I need to gather from the participants?
  - Are the question/s and response options suitable for the biological sex and gender identity data collection requirements I need to gather?
-

# MRS Best Practice Guide on Collecting Data on Biological Sex and Gender Identity

---



## Response Options

- Can the gender identity and biological sex responses be optional?
  - Has the phrasing of the preamble, questionnaire and response options for the biological sex and gender identity data reflected participants who do not understand or appreciate gender identity issues?
  - What response options should I provide?
-

## **MRS Best Practice Guide on Collecting Data on Biological Sex and Gender Identity**

---



- Should I provide closed categories for response options or open fields be provided?
  - Are 'don't know' and 'prefer not to say' options included in the response options?
  - Should the response options be alphabetised or put in random order to reduce potential bias?
-

# MRS Best Practice Guide on Collecting Data on Biological Sex and Gender Identity

---



## Vulnerability

- Are the participants from whom gender identity data is being collected likely to be vulnerable?
- If there are vulnerable participants, has the [MRS Best Practice Guide on Research Participant Vulnerability](#) been referred to?

## Reporting

- Does the report detail the characteristics and parameters used for determining any representative samples e.g., Nat Rep or City Rep samples?
  - Does the report contain sufficient information to determine the validity of any results reported, including sampling parameters?
-



## Guidance timeline

---

**MRS Best Practice Guide on Accessible Data Collection Activities** is available now available in the Standards area of the MRS website

<https://www.mrs.org.uk/pdf/MRS%20Best%20Practice%20Guide%20on%20Accessible%20Data.pdf>

The updated **MRS Guidance on how to read Opinion Polls** and the updated **MRS Best Practice Guide on Collecting Data on Biological Sex and Gender Identity** will be published on the MRS website during November 2025

**Look out for the updated MRS Code of Conduct in 2026!**

---



**Thank you**

If you have any queries please  
contact: [codeline@mrs.org.uk](mailto:codeline@mrs.org.uk)