



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

Kaleke Kolawole
Policy Manager

3

Codeline hot topics and
other new MRS guidance

Julie Corney
**Standards & Compliance
Manager**

Employment Rights Act 2025 - Update



- The Employment Rights Act 2025 has been finalised and received royal Assent on 18 December 2025
 - The Act is being implemented in phases across 2026 and 2027 to give employers time to prepare for the new rights and obligations
 - The first changes begin in early 2026 including:
 - Day one rights to paternity and ordinary parental leave, removing long qualifying periods
 - Statutory Sick Pay payable from the first day of illness
 - Doubling of maximum redundancy protective awards from 90 days' pay to 180 days' pay
 - Establishment of the Fair Work Agency to enforce core workplace rights
 - Expanded whistleblowing protections
-

Employment Rights Act 2025 - Update



- The next wave of changes are planned for October 2026 including:
 - changes to harassment prevention duties
 - extended tribunal time limits
 - Strengthening of safeguards for dismissal-and-rehire practices
 - From 2027 further changes include:
 - a reduced six-month qualifying period for unfair dismissal claims
 - enhanced flexible working rights
 - changes to zero-hour contracts
 - the introduction of a statutory bereavement leave
 - the removal of the unfair dismissal compensation cap
 - A consultation is due in 2026 for the secondary legislation which will underpin the Act – during this, MRS will be pushing for greater clarity regarding the scope of the zero-hour contracts changes
-

Cyber Security and Resilience Bill



-
- The Cyber Security and Resilience Bill is at the Committee stage in the House of Commons
 - The Cyber Security and Resilience Bill reforms and adds to the existing Network and Information Systems (NIS) Regulations 2018, to increase UK cyber defences, and protect essential public services and the broader digital economy from cyber criminals and state-sponsored threats
 - The Bill aims to expand and strengthen the UK's cyber security framework to better protect critical national infrastructure and essential digital services - including healthcare, transport, energy, and water - against growing cyber threats
 - The remit of existing regulations will be widened to cover more digital services and supply chains, which are increasingly exploited by attackers
-

Cyber Security and Resilience Bill



- The Regulators will be placed on a stronger footing to ensure essential cyber safety measures are implemented
 - This includes potential cost recovery mechanisms to fund oversight and new powers to proactively investigate vulnerabilities
 - Organisations will face expanded reporting requirements to give government better visibility of cyber threats
 - The Secretary of State for Science, Innovation and Technology will gain authority to direct regulators and critical organisations (such as NHS trusts or Thames Water) to take specific, proportionate steps to prevent or mitigate cyber attacks
 - 50 percent of UK small businesses reported a cyber attack in the past year with 35 percent of micro businesses experienced phishing attempts
 - Research shows the average cost of a significant cyber-attack in the UK is now over £190k - around £14.7bn a year across the economy - equivalent to 0.5 percent of the UK's GDP
-

Cyber Security and Resilience Tools



- There are some tools freely available to help businesses with cyber security issues including:
 - Cyber Action Toolkit which has been developed by the National Cyber Security Centre (NCSC) which helps strengthen cyber hygiene step-by-step and is designed specifically for non-technical users: <https://cybertoolkit.service.ncsc.gov.uk/>
 - Cyber Essentials Certification a nationally recognised minimum standards for cyber security which protects against the most common types of attacks which includes free cyber insurance, a 24/7 helpline and once achieved gives eligibility for government contracts
 - Cyber reporting via Report Fraud: <https://www.reportfraud.police.uk/>
-

ICO Consultations – international transfers



- The ICO have updated and enhanced its guidance on international transfers of personal information, with the aim of making it quicker for businesses to understand and comply with the transfer rules under UK GDPR
 - The streamlined guidance sets out a clear 'three step test' for organisations to use to identify if they are making restricted transfers
 - The ICO have also added new content on roles and responsibilities, which reflects the complexity of multi-layered transfer scenarios
 - In addition, there are supporting documents including a brief guide, quick reference FAQs and a Glossary to support organisations which do not have specialist knowledge or experience in making international transfers
 - The ICO plan to add an interactive tool to help organisations identify whether they are making a restricted transfer, and more examples and case studies that reflect the complexity of global transfer scenarios
 - An ICO webinar about data transfers is on 10 March at 10am to 11am:
<https://ico.org.uk/about-the-ico/media-centre/events-and-webinars/2026/01/international-transfer-guidance-webinar/>
-

ICO Consultations – data protection enforcement procedure



- At the end of 2025 the ICO issued a consultation to seek organisations' views on the processes the ICO follows when it suspects a breach of the UK GDPR or the Data Protection Act 2018
 - The Data (Use and Access) Act 2025 (DUAA) includes provisions that amend and add to the ICO's existing powers including new powers to require individuals to answer questions and to require organisations to make arrangements for an approved person to prepare a report about a specified matter
 - The new draft guidance reflects the changes to the ICO's enforcement powers
 - Within the guidance, the ICO clarifies the discounts on fines in cases where there is a settlement:
 - 40% if settled prior to the Notice of Intent
 - 30% if settled before representations on the Notice of Intent
 - and 20% thereafter
 - These are the maximum amounts and decisions would be made on a case-by-case basis
-

ICO Investigations and Enforcement



- Staines Health Group sent excessive medical details about a terminally ill patient to their insurance company
- The patient requested that five years of medical records be sent to them to review, before being sent to the insurer to progress the claim
- Instead of five years medical history being sent to the patient, Staines Health Group sent 23 years of medical records direct to the insurer
- As a result, data released was not adequate, relevant and limited to what was necessary for the purpose for which data was processed
- The patient believed the excessive disclosure of unnecessary medical records led to a reduction in the payout of their claim

Points to Note

- A reprimand was issued
 - There was a delay in reporting the breach to the ICO due to a staff member going on annual leave without sharing the password protection details to enable other staff members to access the details of the complaint
 - Failures of Staines Health Group included a lack of written process for staff to follow when handling insurance requests and a lack of regular refresher data protection training for staff
-



UK Adequacy Recognition

- The European Commission extending the UK's adequacy for GDPR for a further 6 years to 27 December 2031
 - The UK remains the only country which has a fixed period for its adequacy recognition
-



International Update

Kaleke Kolawole





EU Digital Simplification

- On 19 November 2025 the European Commission published the EU Digital Omnibus Package. The package is made up of two proposed omnibus laws:
 - a Regulation on the simplification of the implementation of harmonised rules on artificial intelligence (the "Digital Omnibus on AI"); and
 - a Regulation simplifying and consolidating parts of the EU's digital acquis (common EU Laws), making targeted amendments to data, privacy and cyber laws ("Digital Legislation Omnibus").
 - The proposal represents a major legislative turn designed to modernise and harmonise a digital-era rules across the European Union.
 - The Proposal seeks to streamline existing frameworks, close regulatory gaps and ensure consistent protections and obligations across GDPR, the ePrivacy Directive, the Data Governance Act, and the NIS2 Directive on cybersecurity.
 - The Proposal aims to create a clearer, more coherent regulatory environment for organisations operating across the EU's internal market, while supporting innovation and safeguarding fundamental rights.
-

EU Digital Simplification: Overview of Key Instruments



Article 4 of GDPR: Definitions

Personal Data

- This proposal aligns with the recent judgment issued by the Court of Justice (EDPS vs SRB) of the European Union, which found that pseudonymised data will not be personal data in all circumstances.
- The proposal sets out that personal data will be context specific and requires an assessment of all the means reasonably likely to be used to identify the individual.
- This creates a clearer, more coherent regulatory environment for organisations operating across the EU's internal market, while supporting innovation and safeguarding fundamental rights.

Potential Impact

- This proposal introduces a practical, risk-based identifiability test for controllers and recipients. This may facilitate data sharing and analytics in situations where the re-identification risk is demonstrably lower for the recipient. The Commission and/or the EDPB will develop criteria to determine when pseudonymised data can be treated as non-personal for specific entities.
-

EU Digital Simplification: Overview of Key Instruments



Article 4 of GDPR: Definitions

Broader Definition of Research

- The Proposal clarifies the concept of “scientific research”, explicitly recognising commercial research as a legitimate scientific activity under EU law. This mirrors the clarification provided in the UK’s Data Use and Access Act (DUAA), which broadened the scope of scientific research to include commercial research.

Potential Impact

- This change broadens the scope of scientific research to explicitly include commercial activities. In turn this will provide confidence for market researchers, in enacting research provisions and benefiting from the same legal privileges as academic research
-

EU Digital Simplification: Overview of Key Instruments



Article 5(1)(b) of GDPR: Purpose Limitation

Digital Omnibus Proposal Reference: Article 3, Point 2

- The proposal updates the purpose-limitation principle that restricts organisations from using personal data for purposes that differ from the original purpose for collection unless certain conditions are met (Article 6(4)). This has long been an ambiguous area for those undertaking scientific, statistical or historical research activities.
- The proposal clarifies this grey area by stating that further processing for archiving in the public interest, scientific or historical research, or statistical purposes is *automatically* considered compatible with the original purpose. This removes the need to conduct the Article 6(4) compatibility assessment.

Potential Impact

- The proposal brings more clarity to scientific and archival purposes as being compatible with the initial purposes, independent of Article 6(4)
-

EU Digital Simplification: Overview of Key Instruments



Article. 35 of GDPR: Data Protection Impact Assessment

Digital Omnibus Proposal Reference: Article 3, Point 9

- The proposal introduces EU-level harmonisation of data protection impact assessment (DPIA) requirements. The European Data Protection Board (EDPB) would be tasked with drafting three items for the Commission: (i) a list of processing operations that require a DPIA, (ii) a list of operations that do not require one, and (iii) a common EU template and methodology for conducting DPIAs.

Potential Impact

- The proposal would introduce EU-level lists of processing operations that do and do not require a data protection impact assessment (the “no-go list” and “go list”), alongside a common EU-wide DPIA template and methodology.
 - The proposal would enable stronger harmonisation across the EU; greater predictability in risk assessment scoping, and organisations can standardise DPIA practices across jurisdictions.
-

EU Digital Simplification: Overview of Key Instruments



New Article: 88a

Storing of personal data or accessing to personal data stored in terminal equipment of natural persons (cookies/trackers)

- The proposal introduces a clearer, more harmonised approach to determining when organisations may rely on legitimate interests, particularly in contexts involving digital service delivery - including, transmitting a message over a network and aggregated information about the usage of an online service for audience measurement
- This mirrors the UK's Data Use and Access Act (DUAA), which expands exceptions to the consent requirement under the Privacy and Electronic Communications Regulations (PECR) for certain non-essential cookies, including those used for statistical purposes.

Potential Impact

- The Proposal consolidates governance for cookies and trackers into a single instrument when personal data is involved. This should streamline interpretation and enforcement and help reduce inconsistencies between overlapping regulatory regimes.
-

EU Digital Simplification: Overview of Key Instruments



New Article: 88c *AI Development and Operation*

- This Article enables personal data to be processed based on the legitimate interests of the controller under Article 6(1)(f) GDPR, where necessary for the development or functioning of an AI system or model (Regulation (EU) 2024/1689), except where other national laws explicitly require the data subjects consent, or where the legitimate interests of the controller are outweighed by the data subject's rights and fundamental freedoms, particularly in the case of children, requiring the protection of personal data.

Potential Impact

- This amendment would provide a structured path for AI training/operation, subject to robust safeguards. The provision requires a lot more clarity and consideration with respect to scraping and accessing large datasets. Organisations can expect alignment with the AI Act and increased scrutiny on data minimisation, and unconditional opt-out.
-



Conclusion

- The EU Digital Omnibus Proposal is open for consultation until 5 March 2026. The MRS, as a Board Member of the European Federation of Market Research Organisations (EFAMRO), will respond to the Proposals, highlighting the importance of proportionate regulatory measures, the continued role and relevance of sector codes, and the ability of research practitioners to innovate responsibly while maintaining public trust, alongside targeted feedback on the proposed provisions.
 - Organisations are encouraged to share any comments or remarks via codeline@mrs.org.uk by Monday 16 February 2026. MRS will publish its final response.
-

EU Commission & UK Adequacy



- On 19 December 2025, the EU Commission renewed the two 2021 adequacy decisions for the free flow of personal data with the United Kingdom.
 - The decisions ensure that personal data can continue flowing freely and safely between the European Economic Area (EEA) and the United Kingdom, as the UK legal framework contains data protection safeguards that are essentially equivalent to those provided by the EU.
 - The new decisions are subject to a sunset clause of six years, running until 27 December 2031, with the possibility to be renewed. The Commission together with representatives of the European Data Protection Board will review the functioning of the adequacy decisions after a period of four years.
-

China Data Protection FAQ's



- On 9 January 2026, the Cyberspace Administration of China (CAC) published an FAQ clarifying key data protection obligations under China's Personal Information Protection Law (PIPL). It focuses on areas where organisations commonly seek guidance and provides practical clarifications on:
 - Definitions of personal and sensitive personal information, helping organisations classify data consistently and apply appropriate safeguards
 - Personal information protection impact assessments (PIPIAs), including specific guidance on when and how to conduct such assessments for facial recognition and other biometric technologies
 - Designation of a person in charge of personal information protection, including when this is required and how to submit the relevant information to the CAC
-

Hong Kong publishes toolkit on AI-generated deepfakes



-
- On 17 December 2025, the Office of the Privacy Commissioner for Personal Data (PCPD)
 - published *Abuse of AI Deepfakes*, a toolkit designed to help schools and parents
 - understand and manage the privacy risks associated with AI-generated synthetic media.
-
- The guide:
 - Provides practical insights into how personal data may be processed in the context of generative AI
 - Identifies key risk areas, such as consent, transparency, and accuracy
 - Sets out risk mitigation strategies for compliance with the Personal Data (Privacy) Ordinance (PDPO)
 - The guidance signals increasing regulatory attention on the governance of synthetic media. Organisations using or encountering AI-generated content are expected to take a proactive approach to oversight, ensuring privacy considerations are embedded into decision-making, controls, and organisational accountability
-

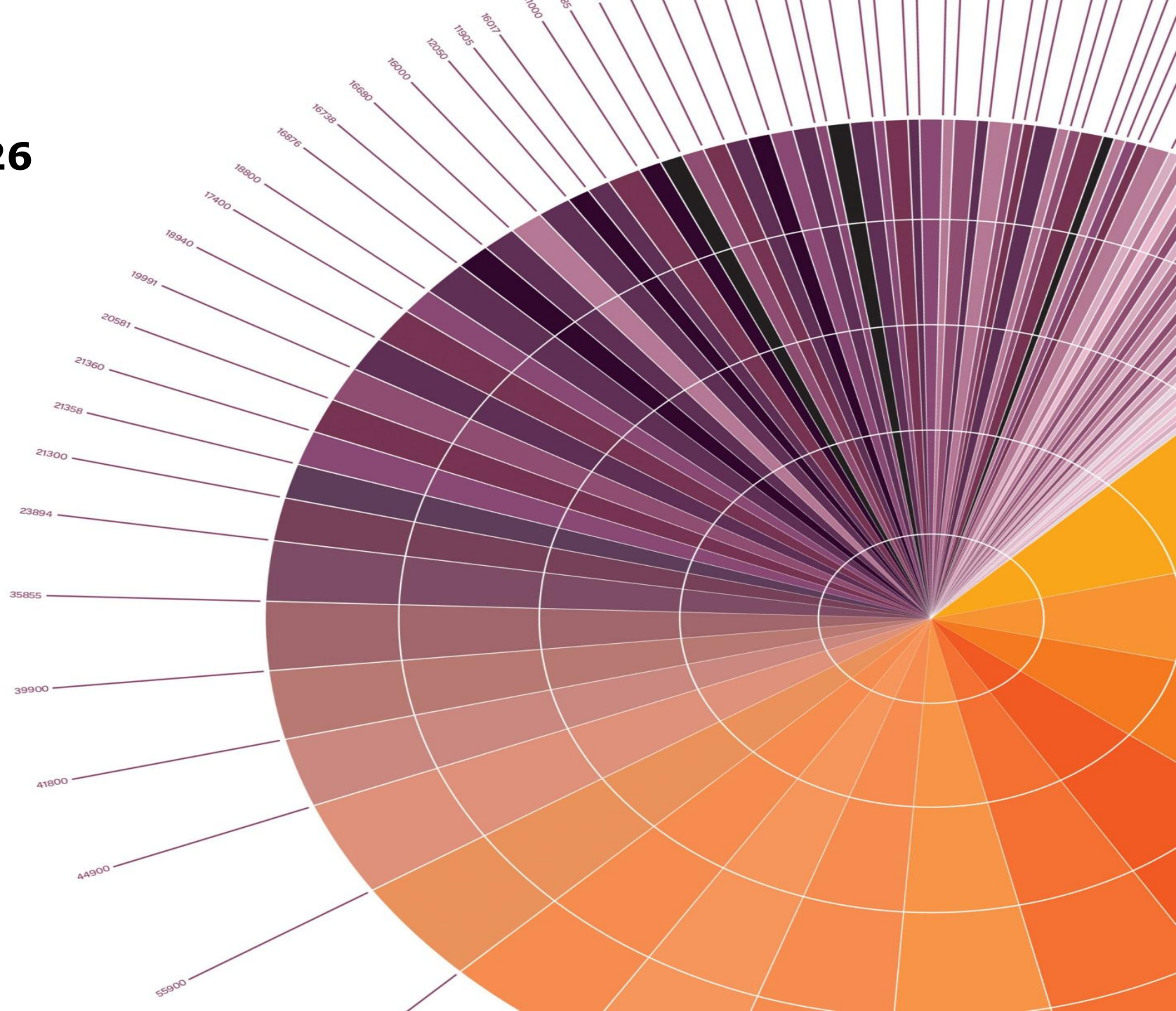


MRS Guidance update

Julie Corney



MRS Code of Conduct – 2026 revision



MRS Code of Conduct 2026 revision



The MRS Code of Conduct is due to be revised during 2026 on its regular three-year revision cycle.

The Code is crucial in helping to protect and regulate first-rate market and social research, insight and data practice. MRS is committed to keeping the Code under regular review to ensure it is fit for purpose.

We plan to start the consultation process with the membership in autumn, with an aim to publish the revised Code at the end of 2026.

MRS Code of Conduct 2026 revision



Members will have the chance to influence the 2026 MRS Code of Conduct revision.

Once the new Code is released, MRS will provide **webinars, briefings, and newsletters** to explain the updates, and there will be a **three-month transition period** from the 2023 Code to the 2026 version. Members are encouraged to **participate in the consultation** and share any suggestions in advance via **codeline@mrs.org.uk**.

MRS Code of Conduct 2026 revision



Areas of change to be considered in the 2026 Code revision:

1. Integration of Technology-related Guidance

The 2026 Code is expected to incorporate or reference the growing **MRS Tech Series** (Metaverse, Biometrics, AI), ensuring the rules reflect current and emerging methodologies.

2. Removal of Outdated or Redundant Rules

A review to strip out any **superfluous or outdated rules** is planned, keeping the Code concise and relevant.

3. Re-structuring the Code

The structure of the Code will be reviewed — particularly whether it still needs to follow the traditional sequence of **planning** → **data collection** → **reporting**.

MRS Code of Conduct 2026 revision



In summary

The 2026 MRS Code of Conduct will likely feature:

- Updated **technology-related rules**
 - A **cleaner, modernised structure**
 - Removal of outdated sections
 - New provisions influenced by **Codeline cases**
-

Research Participant Vulnerability



Research Participant Vulnerability guidance is being updated to incorporate the new BSI standard Suicide and the Workplace (BS 30480:2025), which recognises that suicide affects almost every workplace and provides advisory recommendations for intervention, prevention, and support.

- Suicide-related experiences are common in workplaces.
 - These events have significant adverse impacts, especially when visible or openly discussed.
 - The updated guidance will reflect the need to support individuals and teams affected by such traumatic experiences.
-



Research Participant Vulnerability

The updated Research Participant Vulnerability guidance will also incorporate the Data (Use and Access) Act's (DUAA) recognised legitimate interest — specifically the *safeguarding condition* — which allows the use of personal data when it is necessary to protect the physical, mental, or emotional wellbeing of individuals who need extra support or may be at risk.

At a glance

- The DUAA is a new Act of Parliament that updates some laws about digital information matters.
 - It changes data protection laws in order to promote innovation and economic growth and make things easier for organisations, whilst it still protects people and their rights.
 - Most of the changes offer you an opportunity to do things differently, rather than needing you to make specific changes to comply with the law.
 - The changes will be phased in between June 2025 and June 2026.
-



Research Participant Vulnerability

The safeguarding condition in the Data (Use and Access) Act can only be used when processing personal data is genuinely necessary to protect a “vulnerable individual,” and organisations must meet specific tests to justify this use.

Organisations must:

- Ensure the data use **counts as safeguarding**.
- Confirm the individual is **either a child or an ‘at-risk’ adult**.
- Demonstrate that processing the data is **necessary to safeguard** that person.

It also clarifies what safeguarding means—protecting a vulnerable individual from **neglect or physical, mental or emotional harm**, or protecting their **wellbeing**—and only **one** of these conditions needs to apply.



Research Participant Vulnerability

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’**

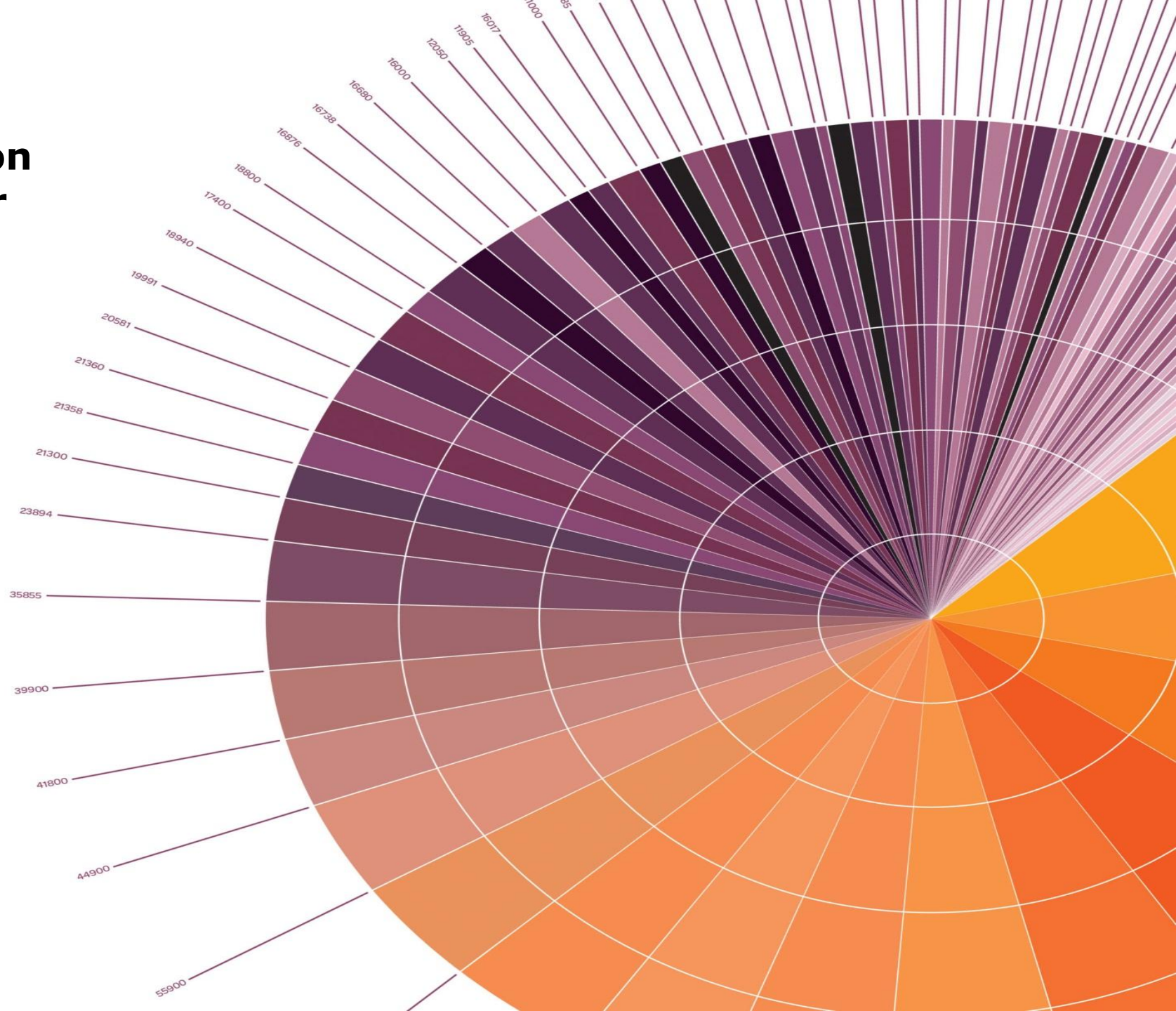
All children and young people under the age of 18 are regarded in this context as “vulnerable”
However, for adults it depends on whether they are ‘at risk’. A person is ‘at risk’ if there is reasonable cause to suspect they:

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

Codeline hot topics

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



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



Researchers must handle the collection of data on **physical disabilities and/or mental health conditions** with **careful preparation and sensitivity**. This includes:

- Providing **clear preamble/context** before asking such questions
 - Being **precise about which categories of data** need to be collected
 - Grouping all related questions **together**
 - Encouraging clients to think carefully about the **level of detail** actually required
 - Ensuring the **privacy of participants** is respected
-

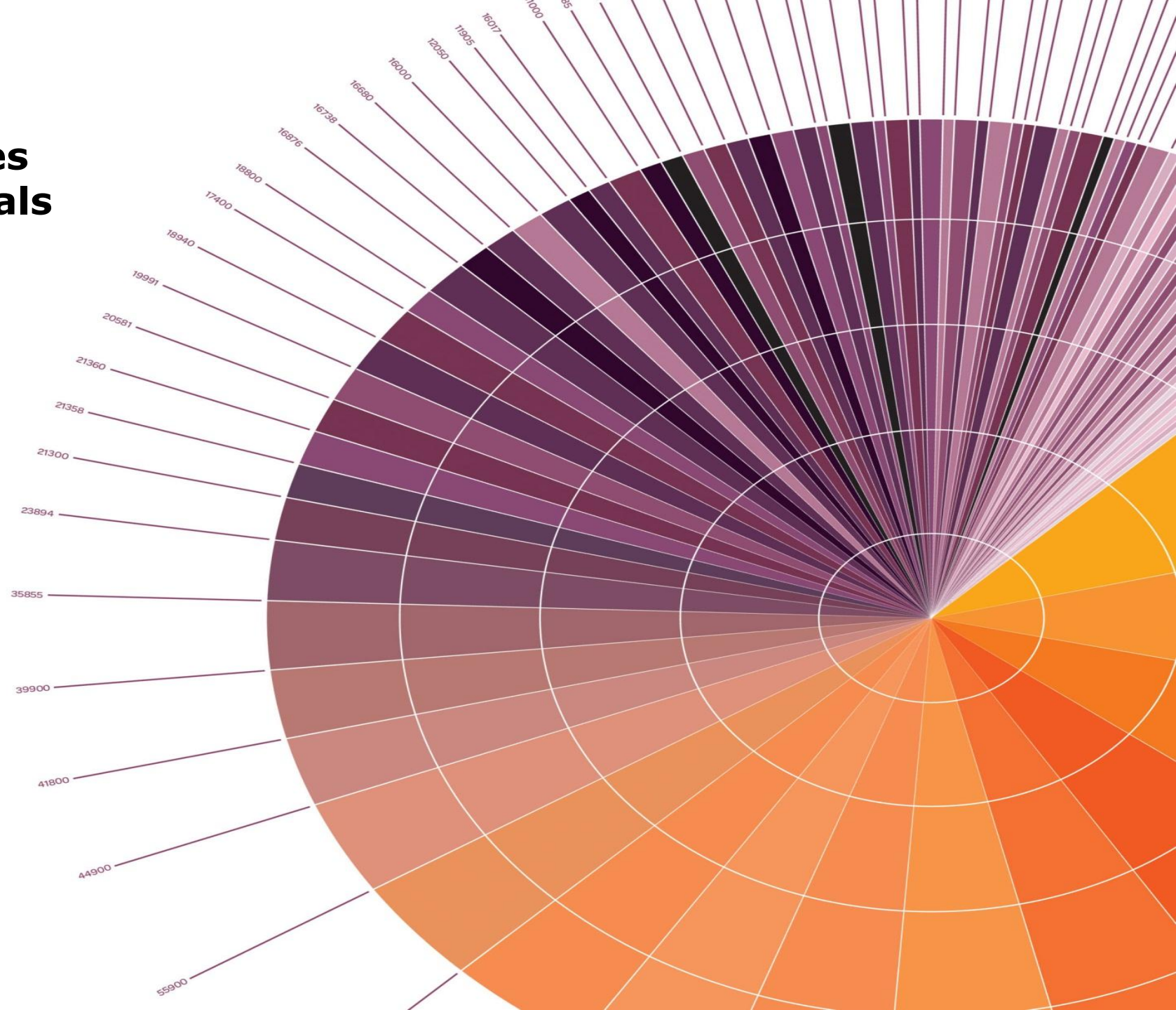
Collecting Sample Data on Physical Disabilities and/or Mental Health Conditions



- **Only collect what is genuinely necessary**, avoiding intrusive or excessive questioning.
- **Provide a clear privacy notice** so participants understand how their data will be used.
- **Allow open responses** where appropriate, giving participants control over how much they share.
- **Offer additional guidance** to help participants respond comfortably and safely.

In summary: **be sensitive, transparent, and proportionate to protect participant dignity while still meeting research needs**

Codeline hot topics
2. Conducting data activities
with neurodiverse individuals



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



1. Accessibility

Researchers should anticipate and remove barriers that may prevent neurodiverse participants from engaging fully. This includes:

- Adjusting the environment for sensory comfort (e.g., lighting, noise, space).
 - Allowing extra time for processing information or completing tasks.
 - Providing materials in multiple formats (visual, written, spoken).
 - These considerations help create a research space that participants can navigate comfortably.
-

Essential Safeguards series: Conducting data activities with neurodiverse individuals



2. Communication

Communication styles vary widely among neurodiverse individuals, so researchers should:

- Use clear, plain language and avoid ambiguity.
 - Offer instructions in several formats (verbal + written).
 - Pause for processing and provide opportunities for questions.
 - This ensures participants can understand what's being asked without unnecessary stress.
-

Essential Safeguards series: Conducting data activities with neurodiverse individuals



3. Inclusivity

An inclusive session is one where every participant feels considered and respected. This includes:

- Tailoring tasks so they are achievable for different cognitive styles.
- Avoiding assumptions about abilities and preferences.
- Ensuring that participation options are flexible (e.g., allowing typed instead of spoken responses).

Inclusivity makes participation feel safe and empowering.

Essential Safeguards series: Conducting data activities with neurodiverse individuals



4. Plan Session Stimulus Thoughtfully

Stimulus materials (e.g., concept boards, prototypes, questionnaires) should be:

- Simple in design and free from unnecessary sensory load.
 - Broken into manageable steps.
 - Predictable in structure to reduce cognitive overwhelm.
 - Planning materials this way supports engagement and reduces anxiety.
-

Essential Safeguards series: Conducting data activities with neurodiverse individuals



5. Remove Participation Barriers

Barriers may be practical, cognitive, sensory, or emotional. Removing them could mean:

- Allowing breaks during sessions.
 - Reassuring participants about the format and expectations beforehand.
 - Providing alternative ways to take part (e.g., remote participation, staggered timings).
 - This reduces drop-out risk and improves data quality.
-

Essential Safeguards series: Conducting data activities with neurodiverse individuals



6. Make Participants Feel Comfortable

Researchers should:

- Create a calm, supportive atmosphere.
 - Build rapport without pressure.
 - Respect participants' autonomy and preferences (e.g., seating, timing, communication style).
 - A comfortable participant gives more genuine, thoughtful input.
-



Thank you

If you have any queries please
contact: codeline@mrs.org.uk