Revised MRS Fair Data Principles – Explanatory Note and Evidence Matrix (September 2018)

Current Fair Data Principle 1	Revised Fair Data Principle	Explanatory Note (illustrative purposes)	Examples of supporting evidence
Principle 1: We will ensure that all personal data is collected with customers' consent.	**Principle 1: We will ensure that all personal data is processed in line with the expectations of the individuals of our use of their personal data.**	*General:* • This principle focuses on how data is processed (i.e. collected, analysed or otherwise used) within an organisation including the use of artificial intelligence and automated processing techniques. *Audit Note:* • In order to properly assess data collection a scoping and mapping exercise will need to be undertaken to assess when and how data is collected within the organisation. • Audit will be conducted on a risk-based approach, identifying areas where risks to personal data is highest. This might be due to: ➢ The types of data collected. Special category data as defined by EU data protection legislation e.g. race or ethnic original, health, etc. Plus other information that	• Privacy Notice/Policy (i.e. public facing document) • Summaries or copies of any Legitimate Interest Impact Assessments (LIA) • Summaries or copies of any Data Protection Impact Assessments (DPIA) • Details of consumer research assessing customer expectations • Details of explanations provided for automated processing techniques • Details of mandatory registration such as UK ICO Data Protection Register Number for controllers based in the UK • Sample customer service telephone scripts • Online data collection forms • Screenshots of digital journey for customers including details required for individual registration • Screenshots of preference dashboards

		participants would deem sensitive such as financial information. ➢ The types of data subjects from whom data is collected. • Areas where this might apply could include: ➢ Customer service scripts ➢ Complaints processes ➢ Customer purchase, and application forms ➢ Online data collection processes ➢ Social media processes • For example, the following issues would need to be considered: ➢ How and where data is collected within an organisation? ➢ Which of this data is personal data? ➢ What purposes are stated at the time of collection? ➢ How is consent obtained from customers? ➢ Sample across all data collection points to assess whether processes and consents are robust.	

Current Fair Data Principle 2	**Revised Fair Data Principle**	**Explanatory Note (illustrative purposes)**	**Examples of supporting evidence**
Principle 2: We will not use personal data for any purpose other than that for which consent was given, respecting customers' wishes about the use of their data.	**Principle 2:** **We will only use data for specified purposes and be open with individuals about the use of their data, respecting individuals' wishes about the use of their data.**	*General:* • This principle focuses on how data is used within an organisation. *Audit Note:* • Areas where this might apply could include: ➢ Details of teams that use and extract customer data (e.g. organigram) ➢ Data usage protocols ➢ Fair processing notices ➢ Opt-out protocols ➢ Opt-out registers • For example, the following issues would need to be considered: ➢ Which teams within an organisation use and extract customer data? ➢ How the teams within an organisation undertake customer data use and what processes are in place to ensure that personal data is only used for the purposes for which it was collected? ➢ What assurances are given to customers at the time of the data collection?	• Privacy Notice/Policy (i.e. public facing document) • Data Protection Policy (i.e. internal facing policy) • Retention policy and schedules • Screenshots of digital journey for customers including details required for individual registration • Screenshots of preference dashboards • Sector specific information requirements in regulated industries

		➢ Are such assurances are being honoured? ➢ How does an organisation manage its fair processing notices? ➢ How does an organisation manage statutory opt-out registers, such as the Telephone Preference Service and other national equivalents? ➢ Sample different teams' approaches to assess whether all procedures are being adequately followed.	

Current Fair Data Principle 3	Revised Fair Data Principle	Explanatory Note (illustrative purposes)	Examples of supporting evidence
Principle 3: We will make sure that customers have access to their personal data that we hold, and that we tell them how we use it.	**Principle 3:** **We will make sure that individuals have easy access to their personal data that we hold, and that we tell them how we use it and how they can exercise their rights over it.**	*General:* • This principle reflects importance of ensuring accessible and transparent data subject rights. Audit Note: • Areas where this might apply could include: ➢ Notification details ➢ Process for completion, maintenance and updating of notification details ➢ Process for personal data complaints and queries ➢ Log of customer complaints regarding collection and/or use of personal data ➢ Log of subject access requests • For example, the following issues would need to be considered: ➢ Details of an organisations data protection notifications and how the notifications are compiled, maintained and updated.	• Privacy Notice/Policy • Screenshots of preference dashboards • Subject Access Requests (SAR) log • Sector specific information requirements in regulated industries • Details of any public API (application programming interface)

		➢ How are customer complaints and queries about personal data managed and recorded? ➢ How are subject access requests managed? ➢ Sample some queries and complaints to assess whether all procedures are being adequately followed, information relayed was correct and whether requests have been honoured e.g. for data correction, removal, etc.	

Current Fair Data Principle 4	Revised Fair Data Principle	Explanatory Note (illustrative purposes)	Examples of supporting evidence
Principle 4: We will protect personal data and keep it secure and confidential.	**Principle 4:** **We will protect personal data and keep it secure and confidential.**	*General:* • This principle focuses on how data is kept, stored and destroyed. *Audit Note:* • Areas where this might apply could include: ➢ Data security policies ➢ Log of security breaches ➢ Procedure for the reporting of breaches ➢ Procedure for escalating personal data breaches • For example, the following issues would need to be considered: ➢ What are an organisations data security and destruction policies and protocols? ➢ How are these policies and protocols applied across an organisations? ➢ What measures are in place if these are breached? ➢ How are customer complaints about data security investigated? ➢ Sample some past breaches to assess whether all procedures were adequately followed, how the breach was	• Data protection policy • Information security policy • Details of technical and organisational measures in place to ensure that there is adequate security over personal data held in manual or electronic form • Data breach management process including data breach logs and record-keeping • Mechanisms for transfer and sharing of between organisations • Mechanisms for transfer of data by EU organisations outside of the European Economic Area (EEA) e.g. Binding Corporate Rules, Model Clauses • Adherence to third party standards e.g. ISO 27001, Cyber Essentials or HIPAA (Health Insurance Portability and Accountability Act 1996)

		resolved and whether the cause of the breach has been adequately addressed.	

Current Fair Data Principle 5	Revised Fair Data Principle	Explanatory Note (illustrative purposes)	Examples of supporting evidence
Principle 5: We will ensure staff understand that personal data is just that – personal – and ensure that it is treated with respect.	**Principle 5: We will ensure staff and all persons involved with our organisation understand that personal data is just that – personal – and ensure that it is treated ethically and with respect.**	*General:* • This principle focuses on how staff – whether employees, freelancers, casual workers, interns or temporary/agency workers – understand their data obligations. *Audit Note:* • Areas where this might apply could include: ➢ Staff Handbook, examples of contracts for non-employees, etc. ➢ Log of personal data breaches by staff • For example, the following issues would need to be considered: ➢ What procedures are in place to commit staff to an organisations data and data protection policies e.g. Handbooks, appraisal requirements, etc.? ➢ What procedures are in place if staff breach personal data processes?	• Data protection policy • Staff Handbook • Staff data protection training materials and induction materials • Training arrangements or assurances provided for other contractors/freelancers • Sample contracts for consultants/freelancers • Testing programmes for staff

		➢ Sample some past breaches to assess whether all procedures were adequately followed, how the breach was resolved and whether the cause of the breach has been adequately addressed.	

Current Fair Data Principle 6	Revised Fair Data Principle	Explanatory Note (illustrative purposes)	Examples of supporting evidence
Principle 6: We will ensure that the vulnerable and under-age are properly protected by the processes we use for data collection.	**Principle 6: We will ensure that the vulnerable and under-age are properly protected by the processes we use for data collection, use and management.**	*General:* • This principle focuses on how more vulnerable members of society are protected. Vulnerability is a complex, dynamic state that can affect anyone at any time and includes permanent, fluctuating and short-term vulnerabilities. *Audit Note:* • Areas where this might apply could include: ➢ Protocols and procedures for collecting personal data from children and vulnerable members of society ➢ Log of any complaints or queries which relate to these segments of customers • For example, the following issues would need to be considered: ➢ What are an organisations policies for collecting and using data from children?	• Evidence of age appropriate design and tailoring for audience such as in Privacy Notices/Policies • Data Protection Policy with appropriate terms • Specific procedures for collection of data from children and/or vulnerable adults • Age verification mechanisms • Operational guidance for treatment of special category data • Template of records required for special category data processing

		➢ What are an organisations policies for collecting and using data from the vulnerable e.g. elderly customers, those with physical or mental health issues, etc.? ➢ How does an organisation target these groups? ➢ Sample some data collection and usage approaches focusing on these groups to assess whether protocols and procedures are being correctly followed.	
Current Fair Data Principle 7	**Revised Fair Data Principle**	**Explanatory Note (illustrative purposes)**	**Examples of supporting evidence**
Principle 7: We will manage our data supply chain to the same ethical standards we expect from other suppliers.	**Principle 7:** **We will manage our data supply chain to the same ethical standards we expect from other suppliers.**	*General:* • This principle focuses on how suppliers are monitored to assess whether suppliers adhere to the required ethical standards. *Audit Note:* • Areas where this might apply could include: ➢ Standard contractual clauses for personal data ➢ Log of supplier complaints and queries ➢ Log of personal data breaches by suppliers • For example, the following issues would need to be considered:	• Standard form supplier contracts with data processors and data controllers • Policies for sharing personal data with third parties. • Corporate Social Responsibility (CSR) Policy • Audit processes for breach notification • Inspections of supply chain • Mystery shopping research reports • Data breach or incident logs

		➢ Which suppliers are used within an organisation that process customer personal data? ➢ What processes are in place to ensure that suppliers that process personal data do so in accordance with an organisation’s data requirements? ➢ What measures are in place if suppliers breach such requirements? ➢ How are customer complaints about suppliers investigated? ➢ Sample some past breaches to assess whether all procedures were adequately followed, how the breach was resolved and whether the cause of the breach has been adequately addressed.	

Current Fair Data Principle 8	Revised Fair Data Principle	Explanatory Note (illustrative purposes)	Examples of supporting evidence
Principle 8: We will ensure that ethical best practice in personal data is integral to our procurement process.	**Principle 8:** **We will ensure that ethical best practice in personal data is integral to our procurement process.**	*General:* • This principle focuses on corporate policies and how suppliers are selected and whether ethical standards are maintained throughout the procurement process. *Audit Note:*	• Procurement policy • Corporate Social Responsibility (CSR) Policy • Supplier terms and conditions • Mandatory GDPR contract terms

		• Areas where this might apply could include: ➢ Corporate social responsibility policies ➢ Procurement procedures ➢ Supplier evaluation procedures ➢ Continuous improvement procedures ➢ Supply-chain management ➢ Internal audit • For example, the following issues would need to be considered: ➢ How are the ethical approaches within an organisation determined? ➢ Does an organisation have a corporate social responsibility policy? If so does this cover personal data? ➢ How are suppliers selected? ➢ What measures are applied to evaluate personal data standards within potential suppliers? ➢ How are continuous improvement processes managed and implemented? ➢ How is the data supply-chain managed, monitored and evaluated? ➢ Is there an internal audit process? If so does this cover personal data?	

Current Fair Data Principle 9	Revised Fair Data Principle	Explanatory Note (illustrative purposes)	Examples of supporting evidence
Principle 9: We will ensure that all staff who have access to personal data are properly trained in its use.	**Principle 9: We will ensure that all staff and persons involved with our organisation who have access to personal data are properly trained in its use.**	*General:* - This principle focuses on how staff – whether employees, freelancers, casual workers, interns or temporary/agency workers – are trained to understand their data obligations. *Audit Note:* - Areas where this might apply could include: ➢ Personal data training materials ➢ Personal data induction materials ➢ Processes for training staff across all types e.g. employees, casual workers, placements, interns, etc. ➢ Details of how role change training is undertaken in relation to data - For example, the following issues would need to be considered: ➢ How does an organisation undertake data training across different types of staff e.g. employees, casual workers, interns, temporary/agency workers, etc.?	- Data Protection Policy - Staff Data Protection training material and logs - Induction, refresher, change in roles data protection training

		➢ How are role and responsibility changes managed in terms of ensuring that staff have adequate data training if their role changes? ➢ How are data protection obligations embedded into staff responsibilities e.g. staff contracts, Handbooks, etc.?	

	New Fair Data Principle	Explanatory Note (illustrative purposes)	Examples of supporting evidence
	New Principle 10 **We will ensure that privacy risks are always properly considered and addressed in all our processes, both automated and non-automated, for the collection and use of personal data.**	*General:* • This principle focuses on how an organisation embeds privacy in practice. *Audit Note* • For example, the following issues would need to be considered: ➢ How are impact assessments used particularly in high risk processing? ➢ What controls are placed on access to data? ➢ What IT systems are used to encourage privacy-centric approach i.e. that personal data is automatically protected in all IT systems or business practices, with no added action required by any individual ? ➢ How is privacy integrated within the IT system?	• Data Protection Policy • Details of explanations provided for automated processing techniques • Details of processes for responding to data subject requests • Summaries or copies of any Legitimate Interest Impact Assessments (LIA) • Summaries or copies of any Data Protection Impact Assessments (DPIA), templates and report summaries • Examples of approach to sign off on projects after assessment of risk • Documented consultations with individuals and results

	New Fair Data Principle	Explanatory Note (illustrative purposes)	Examples of supporting evidence
	New Principle 11 We will ensure that we can adequately resource and can demonstrate our responsibility for compliance with data protection requirements.	*General:* • This principle focuses on demonstrable compliance with ethical and legal requirements. *Audit Note* • For example, the following issues would need to be considered: ➢ What documentation including internal records of processing activities is held by the organisation? ➢ Has data mapping been effectively carried out and documented?	• Governance and responsibility for data protection including terns of Data Protection Officer role (if applicable) • Standards certification such as ISO 27001 • Templates for processing records

Current Fair Data Principle 10	**Revised Fair Data Principle**	**Explanatory Note (illustrative purposes)**	**Examples of supporting evidence**
Principle 10: We will not use personal data if there is uncertainty as to whether the Fair Data Principles have been applied.	**Principle 12:** **We will not use personal data if there is uncertainty as to whether the Fair Data Principles have been applied.**	*General* • This principle focuses on how an organisation embeds the ethical use and protection of personal data within the culture of the organisation. *Audit Note* • Areas where this might apply could include: ➢ Corporate social responsibility documents ➢ Main Board reporting lines ➢ Governance structures ➢ Internal audit and monitoring procedures and protocols • For example, the following issues would need to be considered: ➢ How does an organisation's Corporate Social Responsibility address personal data? ➢ What Governance processes are in place to ensure that the Main Board has personal data on its agenda?	• Governance structure with organisational chart showing responsibility for data protection • Details of any appointed Data Protection Officer and terms and conditions to maintain independence and ensure no conflicts of interest • Rationale for non-appointment of Data Protection Officer • Data Protection Policy • Processes and procedure for review and checking of data use

		➢ What internal audit and monitoring policies are undertaken?	