Governance	Contracts & 3rd Parties	Training	DP Risk Management	Lawful Basis	Trade Offs	Statistical Accuracy	Discrimination & Bias	Security & Integrity	Transparency	Data Minimisation	Individual Rights	Human Review
There is an embedded privacy management framework endorsed by senior management that supports the use of AI systems.	There has been a full consideration y of the controller/processor/ joint controller relationship throughout the whole supply chain in the use of Al systems	BUILDER: All key roles in the design, development and testing of Al systems have received appropriate training in data protection and information security.	There is evidence of proactive engagement between a buyer and a builder, and / or a processor and a controller, as part of the procurement process to facilitate an appropriate risk assessment by the buyer or controller.	The most appropriate Article 6 lawful basis (or bases) and Article 9 or 10 condition have been identified for each processing activity within the Al system.	There has been a risk-based approach taken to navigate / analyse potential 'trade-offs' between data protection considerations and individual rights on the one hand and other competing values and interests on the other.	The organisation has methods in place to ensure that the data sets relied on for determining statistical accuracy are accurately and fairly labelled.	There is evidence that the potential for discriminatory outputs has been considered and mitigated prior to the 'go-live' decision.	There has been a thorough assessment of security risks to or in the Al system prior to its implementation to reduce the likelihood of an attack or breach	Appropriate and timely privacy information is provided to individuals.	There is a review of personal data relevance at each stage of system development and training prior to 'go live', including detailed justification for the retention of data and confirmation that irrelevant data have been removed / deleted.	There is evidence of a policy / process for dealing with individual rights (IR) requests in the data processing pipeline	Human reviewers have appropriate knowledge and experience, authority and independence within the organisation to challenge decisions.
<ol> <li>Technical and operational roles and responsibilities have been assigned to support the day to day management of all aspects of Al systems</li> </ol>	<ol> <li>The decision reached on the controller / processor relationship across all proposed processing activities is documented.</li> </ol>	2. BUILDER: There is appropriate technical training delivered to staff in data protection and privacy roles (e.g. to the DPO, IG Team, risk managers, audit) to ensure they have the appropriate level of knowledge to assess privacy implications and risks during the design, development and testing of their organisations AI system.	<ol> <li>The purpose of the AI system and the most important criteria in the system specification and testing has been considered and documented within a DPIA.</li> </ol>	<ol> <li>A legitimate interests assessment has been undertaken where there is a reliance on legitimate interests as a lawful basis.</li> </ol>	off analysis have been documented	2. There is pre-implementation statistical accuracy testing of new Al systems or changes to existing systems prior to go-live which is documented in a 'test plan'. The decision making process to go-live is documented and includes confirmation that the organisation's required statistical accuracy level has been achieved.	<ol> <li>There is evidence that consideration has been given to including protected characteristics in the system design (if applicable) to ensure fairness / positive action / equity of outcome.</li> </ol>	<ol> <li>Security measures are in place to prevent privacy attacks on Machine Learning (ML) models through model inversion or membership inference.</li> </ol>	2. If personal data is obtained from other sources, all necessary parties can demonstrate compliance with the transparency requirements set out under Article 14 of the UK UKGDPR (unless a relevant exemption applies)	<ol> <li>There is ongoing monitoring and testing of data use to ensure only the minimum data required is being processed by the Al system.</li> </ol>	There is documented guidance available for data subjects on how to make a request.	There is a process in place to ensure periodic assessments of the outcomes of human reviews of the Al system(s) and these assessments take place in practice.
<ol> <li>Privacy considerations and measures for Al development and implementation are set out in a framework of policies and procedures.</li> </ol>	There is evidence that due diligence checks have been completed by all parties to provide assurances that, for the data processed at each stage of the supply chain, individuals have been informed how their data will be used and that it will be passed throughout the chain.	There is evidence that the recruitment process includes a consideration of an applicants existing skills and knowledge and that they are adequately qualified for the role.	of an effective DPIA that meets the requirements under the UKGDPR	3. There is evidence to support that where special category data is used to carry out solely automated decision making within AI systems individuals have provided their explicit consent or an assessment has been completed to determine the processing is necessary for reasons of substantial public interest. Any special category data accidentally created is deleted.	development, there has been a documented assessment to balance the trade off between the level of human work and automation (with the only human interaction being one of human review).	The organisation has processes in place to ensure human review is undertaken, with spot checks being carried out pre deployment and periodically thereafter, with a procedure for triggering a more comprehensive human review if issues are identified, in order to mitigate issues with selection bias or attempts to spoof the controls.	Privacy risks and impacts of a particular technology are evaluated independently by staff with relevant privacy and technical responsibilities for the potential for discriminatory outputs.	Al system for software vulnerabilities Security fixes are applied where	Existing AI privacy information is regularly reviewed and, where necessary, updated appropriately.	There is a process in place to detect unnecessary duplicated data and track data duplication, for example automated data tracing.     This data is deleted where necessary.	There is evidence to confirm that data indexing / tracing and making systems searchable has been considered as part of the system design to effectively respond to requests within statutory timeframes.	The organisation has documented controls in place to prevent their human review practices from introducing deficiencies or errors into the future decision making by the Al system.
The organisation has considered a programme of external audit with a view to enhancing the control environment in place around data processing and security within AI systems		maintain up to date skills and knowledge to enable them to effectively fulfil their responsibilities in their role(s).		4. Analysis has been completed to determine if the results of automated decision making within AI systems could cause legal or other similar effects on the data subject. Considerations has been given to Article 22.2 (a)-(b), Appropriate safeguards have been put in place accordingly.	As part of ongoing system performance monitoring and quality assurance checks, there is evidence of a periodic review of emerging or new trade-offs that could arise should new considerations emerge.	Post-implementation testing is carried out and the results of the testing and action(s) taken as a result are documented.	Al system to ensure there are no	The organisation regularly tests, assesses and evaluates the effectiveness of any data security measures they have put in place (e.g. through techniques such as penetration testing).	Fair processing policies and privacy information are understood by all staff and there is periodic training provided to front line staff whose role includes the collection of personal data for use in Al systems of a regular basis.	There is a documented retention policy / schedule in place and evidence that the schedule is adhered to (personal data is deleted in line with the schedule or retention outside of schedule is justified and approved).	The organisation systematically monitors the time taken to respond to requests in order to identify systems which are potentially more complex.	Where a review identifies that the decision is not correct there is another system or process in place to invoke an alternative method of achieving results (and take the place of the AI system if its competency is questioned).
<ol> <li>There is a programme of risk- based internal audit in place to periodically assess AI systems compliance with data protection legislation and internal privacy policies.</li> </ol>	5. There is an appropriate level of due diligence undertaken prior to any arrangement being agreed to ensure that appropriate security measures will be in place to protect the confidentiality and integrity of personal data within Al systems.	1	5. There is evidence that internal stakeholders, technical specialists within Al product teams and data subjects (or their nominated representative(s)) have been consulted as part of the DPIA assessment as appropriate.	5. There are processes in place to identify the potential use or processing of children's data in Al systems and children's data is not used unless there is a lawful basis to do so.	<ol> <li>Any trade offs considered within data labelling processes have been documented and signed off at an appropriate level / role.</li> </ol>	5. There is evidence that (when received) any complaints regarding inaccurate outputs from AI systems are documented, in particular, any relating to Article 22, including the action taken as a result.	5. Where discriminatory outputs or decisions are identified as part of ongoing monitoring, there is a process in place to deal with or escalate any issues.	5. There is evidence of a policy / process for the separation of the AI development environment from the rest of the IT network / infrastructure. There is evidence that the separation has been adhered to / happened.		,	5. There is evidence that requests relating to decisions made through purely automated means which have a legal or similarly significant effects on individuals are logged, reviewed and actioned appropriately	
Change management processes are documented in policy to ensure that new versions or change releases to AI systems are managed effectively by all parties	6. There is an appropriate level of due diligence undertaken prior to any sarrangement being agreed to ensure that appropriate measures will be in place to protect and enable individual rights	testing, deployment and monitoring of AI systems are adequately qualified to understand the associated statistical accuracy requirements and measures	Appropriate senior management have oversight of completed DPIA reports and sign off on the outcome of the assessment.	<ol> <li>Processes are in place to ensure that marketing to data subjects as a result of profiling within AI systems is lawful.</li> </ol>			Processes are in place to combat any new privacy issues that may be triggered as a result of testing for bias and discrimination.	The organisation has effective asset management processes in plact to ensure a coordinated approach to the security of data within it's systems.			6. There is a process and the technical capability in place to action any requests by individual's to cease processing their data within the Al system(s).	
7. There is a process of communication within the change management process so that all parties understand the impacts of the change(s) and are able to reassess any potential privacy implications.	1 ' ' '	<ol> <li>There is evidence that Al developers and human reviewers are adequately qualified to identify and address bias and discrimination in Al systems.</li> </ol>	manage any risks identified.	7. BUILDER: There is a comprehensive and effective approach in place to ensure data has not been repurposed beyond its original purpose, or that there has been a change in lawful basis within the data supply chain in order to build or train the underlying technology.				<ol> <li>There is evidence that contracts with third parties are clear about the data security role and responsibilities of third parties and that these are implemented and monitored.</li> </ol>			<ol> <li>There is a process and the technical capability in place to action any requests by individual's to erase their data within the AI system(s).</li> </ol>	
<ol> <li>Data flows across the entire supply chain have been comprehensively mapped.</li> </ol>	When procuring AI systems or services, there is evidence that the buyer has completed due diligence to ensure any bias and discrimination in the system has been identified and addressed (where possible).	on the requirement to consider	There are reviews of the DPIA(s) at periodic intervals and when there is a change to processing to ensure it remains accurate and up to date.					There is evidence of a policy / processes for data breach reporting and escalation.				-
	When procuring AI systems or services, there is evidence that the buyer has completed an independent evaluation of any 'trade off' decisions made by the builder when designing the system as part of the due diligence process.	appropriate SOPs / procedures in	There is an effective risk management strategy in place to facilitate the formal documentation of risks associated with the use of Al systems and ensure they are tracked and managed at a corporate level through an appropriate risk register		-			The organisation monitors systems/network activity to detect suspicious requests and take action as a result.				
	10. There are written contracts in place between controllers and processors and 3rd party suppliers / outsource companies which set out the roles and responsibilities of each party and details of the processing taking place.	data protection and privacy roles (e.g. to the DPO, IG Team, risk managers, audit) to ensure they have	10. There is evidence that risks are being mitigated through ongoing AI system development / enhancements					10. When collecting personal data, the organisation has effective measures in place to ensure the data gathered is secured at the point of collection and in transit and to mitigate any security and integrity risks associated with the data gathering.				
	Contracts are managed and reviewed  12. Written contracts include all the	-		•				11. The organisation has in place effective mechanisms in order to prevent unauthorised access (read/write), or inappropriate changes being made to data sets.  12. The organisation has in place				
	details, terms and clauses required under the UK UKGDPR  13. There is in-life contract monitoring or one-off arrangement reviews to ensure partners abide by agreements  PROCESSOR ONLY							effective mechanisms in order to monitor and track all changes being made to personal data. 13. There are business continuity and disaster recovery plans in place.				

1. Data is only processed on the documented instructions of a controller and there is a written contract setting out the respective responsibilities and liabilities of the controller and processor.

2. The processor has taken necessary steps, prior to any arrangement being agreed, to ensure that (within the requirements set out in Contract) they are able to implement appropriate measures to protect and enable individual rights, meet the required security arrangements and provide appropriate privacy information as required.