Control	Control Objective	Risk	Indicators	Suggested Evidences or Documentation
1. There is an embedded privacy management framework endorsed by senior management that supports the use of AI systems.	**Buyer** - To ensure there is effective and clearly defined oversight of data protection compliance to support the use of AI systems purchased by the organisation. Tone from the top - Culture / effective control environment, allowing well informed decision making. **Builder** - To ensure there is effective and clearly defined oversight of data protection compliance to support the development of AI systems. Tone from the top - Culture / effective control environment, privacy-by design, data protection by design and default.	Lack of management focus on data protection when making decisions in the use of AI. Senior management unable to respond to breaches, and not accountable. Non compliance with UKGDPR Article 5 (2), Accountability Principle.	There is an overall governance and privacy management strategy / framework in place that supports the compliant use of AI systems. The framework includes appropriate technical and organisational measures designed to implement the data protection principles in an effective manner Documentation provides evidence that senior management are accountable for understanding and addressing the risks associated with the use of AI appropriately. There is a Data Protection Officer (or a nominated DP lead) in place with designated responsibility which includes oversight of AI systems. There is a Steering Group, Committee, Meeting or equivalent, in place, which is responsible for providing the general oversight for AI systems, their use and the associated data risks within the organisation.	Privacy Accountability Framework. Various job descriptions - privacy personnel, technical staff (designers, researchers, developers etc), senior management, internal audit / compliance staff, procurement staff. DPO job description. Organisational charts Meeting terms of reference for meetings where data privacy is discussed, or that are attended by privacy personnel. Meeting minutes showing data privacy based discussions / actions at various levels within the business, including at senior level. Mission statement, business values or business culture documentation demonstrating management support for data privacy and awareness (tone from
2. Technical and operational roles and responsibilities have been assigned to support the day to day management of all aspects of AI systems	Roles and responsibilities are clearly and systematically defined in job descriptions, team structures and organisation charts	Breaches caused by staff being unaware of their responsibilities. Staff failing to carry out day to day, operational level data protection practices when using AI systems. Non conformance with UKGDPR Article 5 (2).	There are technical and operational roles in place and responsibilities are assigned to ensure the effective management of, and security of data within, AI systems. Responsibility has been assigned in job descriptions to ensure the compliance of the system to data protection legislation	
3. Privacy considerations and measures for AI development and implementation are set out in a framework of policies and procedures.	**Buyer** - There are formal, documented polices and procedures in place that are suitably extensive for the context of the organisation, and provide staff with sufficient direction and rules to follow when managing and deployng purchased AI systems. **Buyer** - There are formalised and documented policies and procedures in place that are suitably extensive for the context of the organisation, and provide staff with sufficient direction and rules to follow when initiating, designing, developing, testing and maintain AI systems.	Policies being miscommunicated when passed on verbally. Staff being unsure of correct procedure, but having no reference material or guidance to check. Breaches because of incorrect assumptions by staff. Operational staff not clear on DP and Organisational requirements leading to data breach. Non conformance with UKGDPR Article 5 (2) and 24.	Policies describe the privacy measures in place for processing that will take place for ongoing training, testing or evaluation of an AI system or service. Policies and procedures are correct, accurate, relevant, representative, complete and up-to-date. There are operational procedures, guidance or manuals in place to support AI policies and provide direction to operational staff on the use of AI systems and the application of data protection law. Policies and procedures clearly outline the roles and responsibilities in the application of the policies.	Privacy or Data Protection policies. Information / Cyber Security policies. Sample Contracts of Employment demonstrating requirement to adhere to privacy and security policies. Procedures containing privacy / data protection elements Design templates containing privacy / data protection elements Design or user manuals containing privacy elements and requirements.
4. 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	That the organisation is carrying out external audit or reviews to provide independent assurances of the effectiveness of the organisation's controls.	A reliance on internal audits and assurances can result in blind spots, causing inaccurate risk assessment and potential breaches. Non conformance with UKGDPR Article 5 (1) (f) and 5 (2)	The organisation completes externally provided self assessment tools to provide assurances on compliance with data protection legislation / information security. The organisation is subject to or employs the services of an external audit provider to provide independent assurances (or certification) on compliance with data protection legislation and information security. The organisation adheres to an appropriate Code of Conduct for their sector.	Audit / External Assessment or Certification Plan Evidence (reports) of completed external audits or certifications e.g. SOC2, ISO27001 etc
5. There is a programme of risk-based internal audit in place to	That there is a programme of internal audits sufficiently detailed for the context of the	Without an audit programme, the organisation can have no assurance that	There is a central Audit plan/schedule in place evidencing the planning of DP based internal audits on an annual basis.	Internal audit plan Internal audit reports

periodically assess AI systems compliance with data protection legislation and internal privacy policies.	organisation. This programme should be appropriately resourced for the context of the organisation. To ensure that the organisation has firstly documented how it will monitor adherence to requirements / rules set out in it's own policies and procedures and then ensures compliance to these requirements through physical routine compliance monitoring.	their risk management is sufficient or effective. If audit findings are not properly reported to oversight and governance bodies, they do not have the correct information to make the necessary decisions, potentially causing breaches. Non conformance with UKGDPR Article 5 (1) (f) and 5 (2) Without ongoing compliance monitoring, controls gradually stop being implemented or may be incorrectly implemented, potentially leading to breaches. Non conformance with UKGDPR Articles 5 (1) (f) and 5 (2).	Audit reports are produced to document the findings from audits undertaken.	
			A central action plan is in place to take forward the outputs from data protection audits.	
			The outputs / reports are shared with the DPO and senior management.	
			Data protection policies and procedures clearly set out how compliance to the policy / procedure will be monitored.	
			Routine compliance checks or audits are then conducted to test staff compliance to data protection policies and procedures.	
6. Change management processes are documented in policy to ensure that new versions or change releases to AI systems are managed effectively by all parties	To ensure that both buyers and builders have documented effective change management processes, which follow the latest guidance and recommended good practice, in relation to change releases and new versions of the system/s.	If there is no effective change management in place, the release of a new system update could cause significant risk of a data breach or damage to personal data if a problem occurs during the release. Non conformance with UKGDPR Article 5 (1) (f) and 5 (2)	Documentation includes measures in place to control the release of any changes / new versions of the system, software reconfiguration, or security patch applications	Product release process. Engineer Design / Product Release Templates Change management logs Historical records of system changes, upgrades, patches applied etc
			Documentation includes a requirement to have an agreed communication plan	
			All changes made, patches applied or new versions released (when and to whom) are recorded / logged and historical information on these changes is easy to locate if required.	
			There is no evidence to suggest overly-frequent updates/releases are happening, as this could suggest a lack of internal checks/sign-off before each one leading to breaches.	
			There is evidence that contracts and contract SLA are reviewed following any significant changes	
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.	**Buyer -** To ensure that the buyer is fully aware of the impact that any changes in the system performance may have on the processing of personal data. **Builder -** To ensure that the builder is keeping their clients aware of how the system is being changed, and the potential impacts that may have on the privacy of their client's data subjects.	Without a proper awareness of how the system is processing personal data, the organisation may be unable to effectively assess or mitigate risks, and will be unable to be accurately transparent regarding their processing activities. Non conformance with UKGDPR Article 5 (1) (f) and 5 (2)	Version releases / changes (including software reconfiguration, or security patch applications) are planned in advance to allow time for the builder to provide education / training to the buyer(s) on what the changes mean in practice	Evidence of release notes on external client facing API site / Developer Hub. Product counselling role job decsriptions. Screnshots of example push notifications - dashboards for clients to view product information, new release information etc.
			Changes, new versions, reconfigurations or patches are not released prior to consultation with buyers	
			Builders actively assist buyers with any updates to existing DPIA	
9. Data flows across the entire supply chain have been comprehensively mapped.	To ensure that both buyers and builders are fully informed about their involvement in the processing of personal data.	Without fully understanding how the data is being processed, neither buyer nor builder can assure themselves that they have an effective information governance regime in place. Non conformance with UKGDPR Article 5 (1) (f), 5 (2) and Article 30.	The organisation has a process to ensure all processing activates are documented accurately and effectively	Data supply chain map Network diagrams - data flow diagram List of sub processors / 3rd party suppliers - includes what data involved, data shared, retention, SCCs. Internal and external facing versions
			Information audits (or data mapping exercises) are conducted to find out how data moves across the supply chain and where data originated from.	
			There is an internal record of all processing activities undertaken by the organisation	

Control	Control Objective	Risk	Indicators	Suggested Evidences or Documentation
1. Appropriate and timely privacy information is provided to individuals.	**Buyer:** To ensure that the buyer has considered their use of AI, has factored it into their privacy notice, and is displaying that privacy information in an appropriate location. **Builder:** To ensure that the builder has made available sufficient information to the buyer to inform the accuracy of their privacy information.	If AI is in use and that is not communicated via privacy information, the organisation is in breach of UKGDPR Article 13, 14 and 22.	The privacy information is concise, transparent, intelligible and uses clear and plain language	Client contract, sales and marketing scripts / clauses Privacy information provided within SDK (screenshots), or website / tool / product / system Privacy Policy Copies of all Privacy Notice / Information Terms of Use / Service Data flow map
			The organisations privacy information or notice includes all the information as required under Article 13 of the UKGDPR.	
			Explanations provided in privacy information are tailored for the intended audience so that they are clear and easy for individuals to understand, taking into account the level of knowledge that the explanation recipient has about the subject.	
			There has been testing done on the interpretability of the privacy information/explanations provided to individuals.	
			Privacy information includes the purposes of the processing and the lawful bases (and the legitimate interests for the processing if applicable).	
			Privacy information includes meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for individuals.	
			Steps have been taken to explain any trade-offs to individuals or any human tasked with reviewing AI output	
			Individuals are provided with privacy information at the time their personal data is collected from them (unless an exemption applies).	
			Individuals are proactively made aware of the information and have an easy way to access it e.g. using a combination of appropriate techniques, such as a layered approach, dashboards, just-in-time notices, icons and mobile and smart device functionalities.	
			Privacy information includes details to enable individual's to challenge the outcome if they think it was flawed (eg if some of the input data was incorrect or irrelevant, or additional data wasn't taken into account that the individual thinks is relevant).	
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)	**Buyer:** To ensure that where the data used for training the AI system is from another organisation and they do not have a direct relationship with the data subject, and where informing them directly would involve disproportionate effort, the buyer ensures that they make this information publicly available, and that the organisations they source the data from have processes in place to inform the data subjects about the processing. **Builder:** To ensure that where the data used for training the AI system is from another organisation and they do not have a direct relationship with the data subject, and where informing them directly would involve disproportionate effort, the builder makes available to the buyer all necessary information to meet their transparency obligations.	The data controller should confirm that appropriate and timely privacy information has been provided to data subjects prior to commencing processing their data in AI systems. There is a risk of breach of the UKGDPR if this is not actioned. Non compliance with Article 14.	Due diligence has been completed with potential data suppliers to confirm appropriate privacy information has been provided to data subjects	Example copies of Client / Customer privacy information or notices
			A DPIA has been carried out to determine whether providing privacy information would involve a disproportionate effort when balanced against the rights and freedoms of individuals	
			If the purpose for using the personal data is different to that for which it was originally obtained, individuals are informed and the lawful basis explained.	
			The privacy information provided includes all the information as set out in Article 14 of the UKGDPR	
			Privacy information includes meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.	
			Privacy information is provided within a reasonable period of obtaining the data, and no later than one month	

3. Existing AI privacy information is regularly reviewed and, where necessary, updated appropriately.	**Buyer** - To ensure that the regular review of AI privacy information is scheduled and documented as part of the contracted service with the supplier of the AI system. **Builder** - To ensure that the organisation engages with any buyers or end point users of its AI products to review and update the privacy information that is provided to data subjects.	If privacy information is out of date, data subjects are not being properly informed of their rights and how their information is being processed. If there is no check on the effectiveness of the communication of privacy information, the organisation has no assurance that data subjects are actually receiving the privacy information. **Non compliance with Articles 13 & 14.**	If the purposes for processing are unclear at the outset, individuals are provided with an indication of what will happen with their data. As processing purposes become clearer, privacy information is updated The privacy information is reviewed against the records of processing activities to ensure it remains up to date and that it actually explains what happens with individuals’ personal data. The organisation carries out user testing to evaluate how effective their privacy information is. A log of historical Privacy Notices is maintained, including the dates on which any changes were made, in order to allow a review of what privacy information was provided to data subjects on what date. The review includes an analysis of complaints from the public about their personal data is used and in particular any complaints about how that use is explained. If there are plans to use personal data for a new purpose within AI processing, there is a process in place to update the privacy information and communicate the changes to individuals before starting any new processing.	Privacy Information Review policy / procedures
4. 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 AI systems on a regular basis.	**Buyer** - To ensure that the organisation can demonstrate that their front line staff are able to explain the necessary privacy information in relation to the use of AI, and provide guidance to any data subject with queries. These staff should have received training to this effect. **Builder** - To ensure that the organisation can demonstrate that they provide the necessary information to their clients, so that their front line staff are able to explain the necessary privacy information in relation to the use of AI, and provide guidance to any data subject with queries. These staff should have received training to this effect.	If front line staff are untrained on privacy information in relation to processing done by AI systems, data subjects may be misdirected or given incorrect information. The organisation is at risk of a breach of UKGDPR Articles 13 & 14.	There is staff training on fair processing and privacy information in There is more specialised / specific training provided to staff working directly with AI systems. Appropriate staff are aware of the various methods or ways in which the organisation provides privacy information.	Privacy / fair processing information training for all staff

Control	Control Objective	Risk	Indicators	Suggested Evidences or Documentation
1. The most appropriate Article 6 lawful basis (or bases) and Article 9 or 10 condition have been identified for each processing activity within the AI system.	To ensure the organsation has documented and concluded its decsion making over the appropriate legal bases under which it processes personal data, special category data or criminal offence data (where necessary).	Without lawful bases identified, documented and included in a privacy notice the organisation may infringe Articles 5, 6, 9 and 10 of the UKGDPR.	Each lawful basis (or bases) and the reasons why they were determined are documented.	Documented lawful basis for each processing activity - e.g. Privacy Notice, RoPA Data flow map Appropriate Policy Document (APD)
			A data flow mapping exercise has been completed to document the data that flows in, around and out of an AI system to ensure a lawful basis is selected for each activity.	
			The DPIA includes a thorough documented and justified assessment of the lawful basis for processing.	
			Where the organisation processes special category data or criminal offence data they have identified and documented a lawful basis for general processing and an additional condition for processing this type of data.	
2. A legitimate interests assessment has been undertaken where there is a reliance on legitimate interests as a lawful basis.	To confirm the organisation holds an LIA which is suitably detailed for the context of the organisation, and which is clearly an honest review of the balance of interests.	Reliance on an inappropriate lawful basis for processing results in potential failure to fulfil the necessary requirements. **Non-compliance with Article 6.**	The LIA includes a consideration of the following: - Not using people’s data in ways they would find intrusive or which could cause them harm, unless there is a very good reason. - If processing children’s data, ensuring extra care is taken to make sure their interests are protected. - Introducing safeguards to reduce the impact where possible. - Whether an opt out can be offered. - Whether a DPIA is required	Legitimate Interest Assessment (LIA)
			The completion of the LIA includes consultation with key technical staff such as system developers	
			The decision and the assessment have been documented clearly	
			The legitimate interests assessment (LIA) was completed prior to the start of the processing	
			The controller has considered that the individual’s interests do not override their legitimate interests as part of the balancing test	
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.	Buyer - Must establish that where an organisation is using AI to carry out automated decision making on, or using special category data, evidence shows that either (a) individuals have provided their explicit consent or (b) the processing is necessary for reasons of substantial public interest prior to any processing having taken place (the conditions set out under Article 22 (4)of the UKGDPR). Builder - Must establish that where an AI is under development that will carry out automated decision making on or using special category data, evidence shows that either (a) individuals have/or will provide their explicit consent or (b) the processing is necessary for reasons of substantial public interest prior to any processing having taken place (the conditions set out under Article 22 (4)of the UKGDPR).	By not having an individual's explicit consent, or being able to demonstrate that the processing is in the substantial public interest, the processing will be unlawful. **Non compliance to Article 6, 9 and 22.**	The controller has a documented assessment of whether the processing is truly automated in nature	Copies of consent statements Consent records log
			A detailed analysis has been carried out of the impact of decision making on data subjects. The analysis also seeks the views of impacted groups or their representatives.	
			Potential legal or similar effects on data subjects with regard to automated decision making have been granularly detailed by the controller. Mitigations and safeguards are documented against each risk.	
			If there is no Article 6 lawful basis or Article 9 condition, special category data is deleted prior to any automated decision making.	
			There has been an assessment of the likelihood of SCD being accidentally created (eg assessing whether any data acts as a good proxy for SCD).	

			If there is no Article 6 lawful basis or Article 9 condition, any special category data created as a result of automated decision making is deleted.	
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.	Buyer - Determine that the controller has considered how the purchased system may allow ADM on data subjects, how far reaching the effects may be and that appropriate safeguards are in place. Builder - Ensure the developer has considered how the system can be used for ADM, how far reaching the effects may be and has put in place appropriate safeguards.	By not carrying out adequate risk assessments to protect data subjects, this could cause significant distress and impact on their rights/freedoms and may place the organisation in breach of Article 22 (1-2) of the UKGDPR.	If there is no Article 6 lawful basis or Article 9 condition, the DC ensures that any AI models being used do not unintendedly infer special category / criminal conviction data	Article 22 assessment
			Where processing is carried out using special category data (such as biometric SCD), additional safeguards have been applied by the controller in the securing of the data.	
			Where an organisation does not have a lawful basis to carry out automated decision making on special category data, any analysis carried out involving this data is in an aggregate format and does not identify individual data subjects.	
5. There are processes in place to identify the potential use or processing of children's data in AI systems and children's data is not used unless there is a lawful basis to do so.	**Buyer -** Establish that where an organisation is processing children's data in AI systems, it has identified a lawful basis to do so prior to any processing and has implemented robust safeguards in line with current guidance. **Builder -** Establish that where an AI is developed with the intention to process children's data, it has identified a lawful basis to do so prior to any processing during the development processes and has implemented robust safeguards in line with current guidance.	Without a lawful basis or robust safeguards there will be a breach of UKGDPR. Non compliance to Article 6	There are systems in place to verify data subjects' ages prior to processing.	DPIA (and LIA if appropriate) covering the processing of children's data
			Where processing is carried out on children's data, there is a documented lawful basis for doing so.	
			Where processing is carried out on children's data, the controller can robustly evidence a necessity to do so (such as an LIA where the basis is legitimate interests)	
			Where processing is carried out on children's data, additional safeguards have been applied by the controller in the securing of the data.	
			Where an organisation does not have a lawful basis to carry out automated decision making on children through AI systems, any analysis carried out involving this data is in an aggregate format and does not identify individual data subjects.	
6. Processes are in place to ensure that marketing to data subjects as a result of profiling within AI systems is lawful.	Establish that where an organisation's marketing activities include the reliance on the outputs of an AI system, all personal data used to facilitate the marketing has been obtained appropriately (in line with the relevant privacy notice) and is processed on an appropriate lawful basis.	By not having a lawful basis to market to data subjects, the organisation is likely to be processing unlawfully which could impact on the data subjects' rights and freedoms, as well as resulting in potential enforcement action. **Non compliance with Article 6.** Consideration of PECR.	The lawful basis as documented in the privacy notice is aligned with how personal data has actually been used for marketing.	
			The lawful basis relied upon for marketing is appropriate.	
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.	All parties must ensure that there is an appropriate and legitimate lawful basis for their ongoing processing of the data (and that no inappropriate change in lawful basis has occurred throughout the supply chain). **Builder -** To ensure that there is due diligence undertaken to confirm that data used to train an AI system is not now being processed for these purposes under a different lawful basis	If there is an inappropriate change in the lawful basis for processing within the supply chain (e.g. data originally collected under consent, now being processed under legitimate interests) then there is a risk that this will be unlawful. Without due diligence / a review to identify the issue, personal	There is a process in place to check the purposes and lawful basis for which data sets were collected and ensure that those purposes or lawful basis have not changed in the development of the AI system.	
			The lawful basis under which each data set was collected (directly or indirectly from a client or broker) are clearly documented and the mapping exercise includes a log of the lawful basis now being used.	

	from which it was originally collected under. To ensure there is an ongoing review of data flows, to provide continued awareness of alterations or changes in any aspect of the processing activities, in order to ensure that there has not been purpose drift during the lifespan of the system. **LINKED TO CONTROL 3 IN CONTRACTS & 3RD PARTIES DOMAIN**	data may be processed for purposes other than those for which is was collected, **in breach of Article 5 (1) (b).**	Where data is not sourced / collected directly by the builder: Due diligence checks are undertaken by the builder when sourcing data with which to train the AI system to check under which lawful basis the data was originally collected and what privacy information was provided to support it's repurpose, and then ensure that there is not a change in lawful basis when the AI builder is using the data to train the system. Where data is not sourced / collected directly by the builder: Due diligence checks include the entire data supply chain. Where data was originally collected by a third party under consent, the buider has checked that the consent statement was clear and granular enough to permit it's ongoing use to train the AI system (and that individual's are aware that their data will be used in this way). A 'fairness' and 'lawfulness' assessment has been conducted as part of the DPIA.	
8. There is evidence of a periodic review of documented lawful bases to ensure their continued validity.	**<u>Buyer</u>** - That there are proactive reviews of the previously documented lawful bases which demonstrate an honest commitment to confirming and refreshing the bases originally selected. **<u>Builder</u>** - That there are proactive reviews of previously documented lawful bases which demonstrate an honest commitment to confirming and refreshing the bases originally selected, particularly if an AI system or componets may be re-used for different purposes than originally intended.	If the lawful bases are not regularly reviewed, the nature of the processing may change sufficiently to no longer be what bases originally processed under. This could place the organisation in breach of UKGDPR Articles 6 and 9.	There is a process in place to review documented lawful bases to check that the relationship, the processing and the purposes have not changed The controller periodically assesses the model usage to ensure purpose remains the same and necessity and legitimate interests (LI) are still valid. The reviews take place on a suitably periodic basis The controller has implemented corrective measures to AI system in order to satisfy the original lawful basis The controller has selected a new lawful basis and associated actions. For example, the controller has carried out a legitimate interests assessment or obtained consent.	Evidence of Lawful Basis reviews

Control measures	Evidences			Assurance	Report Text					QA
	Documentation	Interview	Testing	Rating	Findings	Non Conformities	Recommendations	Priority	Best Practice	QA Comments
Governance										
1. There is an embedded privacy management framework endorsed by senior management that supports the use of AI systems.				Green	hbgivboiu	nfvo inbwfp iowbnf	dvbn owb ow	Urgent		
2. Technical and operational roles and responsibilities have been assigned to support the day to day management of all aspects of AI systems				Yellow		dnbc owowbonwdbwd wd kjwbd nivhwuoihvwuv iuhvwiubvhweouhro iuhv woeruhv wo o	cdbiwudhbgcou hwouwdhuo uoehvcouewhv oow weouihv ohwo	High		
3. Privacy considerations and measures for AI development and implementation are set out in a framework of policies and procedures.				Amber		dwjv howiuhjoeihcnv ldlo vowh bouwhouvhfehvbnbeuhvo viov uv hwowh ohig wuhv hwdiv hwiuhve gouwg owuh iwgiuwe	fjb oue hgv,wrkli iuhr otyhg oe;uthoeh ; iuhrg ;uerh ierggreh glier lierhg luerh gherl	Medium		
4. 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				Red						
5. 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.										
6. Change management processes are documented in policy to ensure that new versions or change releases to AI systems are managed effectively by all parties										
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.										
9. Data flows across the entire supply chain have been comprehensively mapped.				Green						
Transparency										
1. Appropriate and timely privacy information is provided to individuals.				Yellow						
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)										
3. Existing AI privacy information is regularly reviewed and, where necessary, updated appropriately.										
4. 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 AI systems on a regular basis.				Green						
Lawful Basis										
1. The most appropriate Article 6 lawful basis (or bases) and Article 9 or 10 condition have been identified for each processing activity within the AI system.				Yellow						
2. A legitimate interests assessment has been undertaken where there is a reliance on legitimate interests as a lawful basis.										
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.										
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.										
5. There are processes in place to identify the potential use or processing of children's data in AI systems and children's data is not used unless there is a lawful basis to do so.										
6. Processes are in place to ensure that marketing to data subjects as a result of profiling within AI systems is lawful.										
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.										
8. There is evidence of a periodic review of documented lawful bases to ensure their continued validity.				Red				Urgent		

Control	Control Objective	Risk	Indicators	Suggested Evidences or Documentation
1. There has been a full consideration of the controller/processor/ joint controller relationship throughout the whole supply chain in the use of AI systems	To ensure that the controllership of the personal data has been properly considered and accurately determined.	If no determination of controllership has been made, it is likely that all parties will fail to meeting their obligations under many parts of the UKGDPR.	Evidence (e.g. emails, meeting minutes, model design or specification documents) confirms there has been a consideration of the relationship between all parties	Privacy Management Framework documents DPIAs Contracts Data flow mapping System specification documents
			There is a requirement within DPIA templates to assess the relationship	
			Evidence confirms that the whole supply chain has been considered within the assessment	
			Considerations and conclusions are in line with ICO and sectoral / EU guidance on the role of controllers and processors	
			All parties have identified the distinct sets of processing operations and their purposes in order to understand the relationship	
2. The decision reached on the controller / processor relationship across all proposed processing activities is documented.	To ensure that the decision is documented in appropriate documentation or records.	If decisions are not formally documented there is a risk that the agreements reached in this matter will be misunderstood, forgotten or not complied with.	The assessment conducted and the reasons / methods used to determine the decision is documented within DPIA(s)	DPIA Contracts RoPA Privacy information / notice / policy
			The decision is reflected in the RoPA for all processing activities	
			The relationship is formally documented and agreed within Contracts / Agreements	
			The relationship is communicated to individuals in the privacy information	
3. 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.	All parties must ensure that customers who share personal data with them have provided their data subjects with adequate privacy and transparency information, including the details around the sharing process. **LINKED TO CONTROL 7 IN LAWFUL BASIS DOMAIN**	If data subjects are not given sufficient privacy information there is a risk of non-compliance with Articles 13 and 14 of the UKGDPR.	Due diligence checks are documented	Vendor checklists & onboarding risk assessment questionnaire Contracts Checks on supplier reputations, financial standing etc
			The due diligence process includes a check of privacy information currently available / provided by the buyer (Client) of the AI system	
			Due diligence includes checks on business process outsourcing organisations (BPOs) working on behalf of the builder (subcontracted), for example BPOs conducting human review checks	
			It is clear from the privacy information that individuals are aware of the sharing of their data with the AI supplier, the reasons for this (lawful basis), the intended outputs and how to exercise their individual rights.	
			Where privacy information is not yet available due diligence confirms the existence of a process to ensure that this is provided within one month.	
4. Where the use of an AI system results in the creation and therefore processing of new attributable personal or special category data, due diligence checks are undertaken to ensure that individuals have either already received appropriate privacy information or else are provided with it in a timely manner.	All parties must ensure that any new personal or special category data created as a result of the use of AI systems are transparent to the data subject.	If data subjects are not given sufficient privacy information there is a risk of non-compliance with Articles 13 and 14 of the UKGDPR.	Due diligence checks are documented	Due diligence checklists - sample of completed checks Copies of 3rd party, BPO, Client privacy information
			The due diligence process includes a check of privacy information currently available / provided by the supplier of the AI system	
			It is clear from the privacy information that individuals are aware of the sharing of their data by the AI supplier.	
			Where privacy information is not yet available due diligence confirms the existence of a process to ensure that this is provided within one month.	

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 AI systems.	Buyers must ensure they undertake a process of checks and assurances appropriate to the data and risk to ensure supplies have the necessary mechanisms to secure personal data entrusted to them before buying the system	Without adequate security measures there is a risk of non-compliance with Article 5.1.f and Article 32 of the UKGDPR.	Security based due diligence checks are documented	Security assessments or audits
			The due diligence process includes data security checks (site visits, system testing etc).	
6. There is an appropriate level of due diligence undertaken prior to any arrangement being agreed to ensure that appropriate measures will be in place to protect and enable individual rights	Buyers must ensure they undertake a process of checks and assurances to ensure suppliers have the necessary mechanisms to allow data subjects to exercise individuals rights over their personal data	Without adequate measures to allow data subjects to exercise their individual rights, there is a risk of non-compliance with Article 5 and Articles 15-22 of the UKGDPR.	Due diligence checks are documented in DPIAs	Copies of 3rd party, BPO, Client individual rights policies Individual Rights Policies and procedures
			The due diligence process includes checks to confirm a potential processor, 3rd party or outsource company will protect and enable all data subjects rights.	
7. When procuring AI systems or services, there is evidence that the buyer has considered what their acceptable level of system output accuracy is and has completed due diligence to ensure the product meets these accuracy requirements.	To ensure that the buyer has completed due diligence checks with the vendor to gain assurances that accuracy requirements can be achieved generally. Also to ensure the buyer has considered the impacts in accuracy resulting from the use of the system to existing processing, products or services. The buyer should have considered what levels of accuracy are acceptable at the outset and have documented how they will measure these once the system is deployed.	Without first considering what accuracy levels are acceptable and how they can mitigate any inaccuracies that may arise from the outset, there is a risk that unacceptable levels of inaccuracy will be produced that will negatively impact on the outputs and could impact an individual's rights and freedoms. If due diligence is not undertaken there will be no assurances on the systems ability to meet accuracy requirements.	Prior to procurement, there is evidence that the buyer has considered and decided the level of statistical accuracy that they are prepared to accept from the AI system	Outputs of statistical accuracy testing reporting provided as part of procurement process. Quality control checklist - random sample. Outsourced checks.
			Prior to procurement, due diligence has been completed to understand and confirm the level of statistical accuracy that can be expected from the AI system	
			The builder has run and tested the system in 'ghost mode' or in a testing environment to understand accuracy levels.	
			The buyer has reviewed the use of the AI system against existing systems, products or services to ensure that it does not impact on their accuracy outputs by deploying the new AI system	
			Accuracy based KPI / SLA are included in written contracts with third party suppliers	
			Where accuracy levels fall below tolerated levels, there is evidence that services have not been procured.	
8. 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).	To ensure the buyer has undertaken a collaborative process with the builder to understand the risk of discriminatory outcomes and biased decisions making by an AI based on a mutual understanding of the data inputs, the objective of the IA and decision making foundations of the technology.	Without a solid mutual understanding of the risks to individuals around automated decision making there is a risk of non-compliance with Article 22 of the UKGDPR	Prior to procurement, due diligence has been completed to understand the level of bias and discrimination that can be expected from the AI system	Outputs of discrimination / bias testing reporting provided as part of procurement process. Quality control checklist - random sample. Outsourced checks.
			Where bias or discrimination can not be mitigated, there is evidence that services have not been procured.	
9. When procuring AI systems or services, there is evidence that the buyer has	To ensure that when purchasing an AI system, the	Without proper due diligence the data controller may proceed with deployment based	Prior to procurement, due diligence has been completed to understand the trade offs within the AI system	Outputs of any trade off review / reporting provided as part of procurement process.

completed an independent evaluation of any 'trade off' decisions made by the builder when designing the system as part of the due diligence process.	buyer has considered and documented potential trade-off decisions conducted by the vendor, for example individual privacy vs the goal of the AI output.	on inappropriate weighting given to competing priorities	There is a process in place to halt the deployment of any AI systems, if it is not possible to achieve an appropriate trade-off between two or multiple data protection requirements	
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.	To ensure that there are written contracts in place to govern the processing activities that are being done by each party and where the responsibilities lie.	Breach of controller/processor requirements. Non conformance with UKGDPR Articles 28 and 5 (2). May not understand how personal data is being processed by third parties, or may have entered into verbal agreements only, which puts the organisation at risk and without recourse should there be a breach of UKGDPR requirements.	The data controller has identified the distinct sets of processing operations and their purposes in order to understand the relationship	3rd Party Contracts
			Written contracts are in place with all processors	
			The contracts are approved by senior management and signed by both parties.	
			Contracts clearly set out the relationship and decision making boundaries between each party.	
			Contracts clearly set out who in practice decides the purposes and essential means of the processing	
			Roles and responsibilities are documented within standard T's & C's, agreements, contracts or other such documentation	
			The technical controls and settings for the AI system are documented and agreed	
			If a processor uses a sub-processor to assist in its processing of personal data for the organisation, there is written authorisation in place from the organisation and a written contract in place with that sub-processor	
11. Contracts are managed and reviewed	To ensure that the data controller take the necessary steps to appropriately record, review and refresh its contractual agreements according to pre-set	Without a structured approach to contract management there is a risk of non-compliance with Article 28 and Article 30 of the UKGDPR	There is a central record or log of all contracts currently in place	Contracts log / record
			Contracts are reviewed on a periodic basis to ensure they remain up to date	
			The responsibility and timeframes for reviewing contracts has been documented either in the contract itself or in the contract log	
12. Written contracts include all the details, terms and clauses required under the UK UKGDPR	To confirm that all contracts with processors cover the requirements of the UK UKGDPR controller/processor requirements.	Breach of controller/processor requirements. Non conformance with UKGDPR Articles 28 and 5 (2). May lose control over personal data, resulting is loss, disclosure, or other breaches. May be unable to respond to SARs or other individual rights within the statutory deadline.	Each contract (or other legal act) sets out details of the processing including: the subject matter of the processing; the duration of the processing; the nature and purpose of the processing; the type of personal data involved; the categories of data subject; the controller’s obligations and rights	

			The contract or other legal act includes terms or clauses stating that: - the processor must only act on the controller's documented instructions, unless required by law to act without such instructions; - the processor must ensure that people processing the data are subject to a duty of confidence; - the processor must only engage a sub-processor with the controller's prior authorisation and under a written contract; - the processor must take appropriate measures to help the controller respond to requests from individuals to exercise their rights.	
			Contracts include the technical and organisational security measures the processor will adopt (including encryption, minimisation /pseudonymisation, resilience of processing systems and backing up personal data in order to be able to reinstate the system).	
			Clauses are included to ensure the processor must delete or return all personal data to the controller (at the controller's choice) at the end of the contract, and the processor must also delete existing personal data unless the law requires its storage	
			Clauses are included to ensure that the processor must assist the controller in meeting its UKGDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments	
13. There is in-life contract monitoring or one-off arrangement reviews to ensure partners abide by agreements	**<u>Buyer</u>** - To ensure that contract management is an evolving and continuous process with the vendor/supplier, and that the vendor is operating according to contract expectations **<u>Builder</u>** - To ensure cooperation and information exchange with the customer, allowing inspection and audit and responding to any issues that come to light.	If agreed roles and responsibilities between controllers and processors and joint controllers are not being undertaken in practice then there is a risk that documented agreements, T's & C's, or contracts are in breach and that there is a lack of control over who does what in the management of the AI system. **Non conformance with Article 5 (2) and Article 28 (1) & (3).**	There is a documented process for managing the ongoing relationship with data processors / joint controllers / 3rd party suppliers or	Contract review records
			Responsibility for oversight of data processors is formally assigned within the controller's organisation	
			There is evidence of periodic reviews of the practical day to day management of the AI system to provide assurances that the agreed roles and responsibilities are being undertaken and there is no discrepancies or role creep.	
			There is evidence that where role / responsibility 'creep' has occurred that an assessment has been undertaken of existing agreements and changes implemented appropriately	
			Clauses are included within contracts to allow the buyer to conduct audits or checks to confirm the processor / 3rd party / outsource	
			Routine compliance checks are conducted to test that processors / 3rd parties / outsource companies are complying with contractual agreements.	
			The checks are proportionate and appropriate for the risk of processing undertaken.	
PROCESSOR ONLY				

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.	To ensure there is a written contract with the controller that sets out the respective responsibilities and liabilities of the controller processor; and ensure there is a review and amendments made to any existing contracts to ensure they meet the requirements under the UKGDPR.	Breach of controller/processor requirements. Non conformance with UKGDPR Articles 28 and 5 (2). May lose control over personal data, resulting is loss, disclosure, or other breaches. May be unable to respond to SARs or other individual rights within the statutory deadline. If agreed roles and responsibilities between controllers and processors and joint controllers are not being undertaken in practice then there is a risk that documented agreements, T's & C's, or contracts are in breach and that there is a lack of control over who does what in the management of the AI system. Non conformance with Article 5 (2) and Article 28 (1) & (3).	Each contract (or other legal act) sets out details of the processing including: the subject matter of the processing; the duration of the processing; the nature and purpose of the processing; the type of personal data involved; the categories of data subject; the controller's obligations and rights	Processor contracts
			The contract or other legal act includes terms or clauses stating that: - the processor must only act on the controller's documented instructions, unless required by law to act without such instructions; - the processor must ensure that people processing the data are subject to a duty of confidence; - the processor must only engage a sub-processor with the controller's prior authorisation and under a written contract; - the processor must take appropriate measures to help the controller respond to requests from individuals to exercise their rights.	
			Contracts include the technical and organisational security measures the processor will adopt (including encryption, minimisation /pseudonymisation, resilience of processing systems and backing up personal data in order to be able to reinstate the system).	
			Clauses are included to ensure the processor must delete or return all personal data to the controller (at the controller's choice) at the end of the contract, and the processor must also delete existing personal data unless the law requires its storage	
			Clauses are included to ensure that the processor must assist the controller in meeting its UKGDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments	
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.	Processors must ensure they undertake a process of checks and assurances to ensure themselves that they are able to meet the requirements of both the Contract with the controller and the requirements under data protection law.	Although the controller is ultimately liable for overall compliance with the UKGDPR and for demonstrating that compliance, as processor you have some direct responsibilities and liabilities of your own. If processors fail to meet any of these obligations, or act outside or against the instructions of the controller, they may be liable to pay damages in legal proceedings, or be subject to fines or other penalties or corrective measures. Risk of non-compliance with Article 5 and Articles 15-22 of the UKGDPR and Article 28.	Due diligence checks are undertaken and documented prior to contract agreement	Due diligence checks completed by the processor
			The due diligence process includes a check of privacy information currently available / provided by the controller.	
			It is clear from the privacy information that individuals are aware of the sharing of their data by the controller to the processor	
			Where privacy information is not yet available due diligence confirms the existence of a process to ensure that this is provided within one month by both parties.	
			Security based due diligence checks are documented	
			The due diligence process includes checks to confirm data subjects rights can be enabled and protected.	

Control	Control Objective	Risk	Indicators	Suggested Evidences or Documentation
1. 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.	To ensure that the system is built to allow review of personal data relevance by the organisation using the system at each stage of development. To ensure that there has been a consideration of the data being retained and that the purposes that each data set is needed for at each stage of development has been considered and then removed as appropriate. For each stage of development, for example in the training phase where larger data sets may be required, the necessity of retaining such data is justified - at each stage only data that is required is used.	Without appropriate reviews being undertaken at each stage, there is a risk of inappropriate retention of data. **Non compliance with Article 5 (1) (c)**	There has been an assessment of the features used to train the AI system – and therefore what data – are relevant for the purpose, and the design makes sure only that data is processed.	DPIA(s) Principles / values / product brief Design documents Database design maps
			There has been an assessment to ensure the training data can be modified to reduce the extent to which it can be traced back to specific individuals	
			Development plans include specific review phases to check data is being minimised / not retained when no longer needed.	
			The DPIA includes a justification for the retention of data where applicable	
			There is evidence in place to confirm that irrelevant data has been removed or deleted during the system development phase.	
2. There is ongoing monitoring and testing of data use to ensure only the minimum data required is being processed by the AI system.	To ensure that, following deployment, data is monitored and tested to limit use to only that which is required by the system. To ensure there are periodic review(s) of the data used to check it is still relevant / needed e.g. testing against other systems with fewer features or data to see if the same results can be achieved, with a view to reducing the amount of personal data being processed.	If data is not assessed and then separated then there is a risk that excessive data will be processed and retained for longer than is necessary. **Non compliance with Article 5 (1) (c).**	There is a review policy / procedure in place which outlines the key steps that should be taken with specific timeframes.	Data Minimisation policy and procedures Data minimisation test plan and reports
			There is a checklist or test plan in place to standardise the checks required - this includes a check of the current features within the system and a review of retention of data and potential further minimisation of data used.	
			Reviews include an assessment as to whether all the data is needed (for example whole address or just postcode will produce same result) and whether the same volume of data is required (or whether the same results can be achieved with less volume)	
			Reviews include consideragion of document 'cropping' or redaction for both collection and sharing purposes	
			Reviews are documented and shared with all relevant parties	
3. 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.	To ensure that there are processes in place to avoid the creation, processing or retention of unnecessary duplicate data in the system throughout all the various stages of development and deployment. This should also be considered across potentially complex supply chains.	If unnecessary duplicate data is created, processed or stored in the system then there is a risk that the data sets as a whole are excessive. **Non compliance with Article 5 (1) (c).** Due to the inherent complexities of AI systems and their supply chains, without automated data tracing being used it is unlikely that the organisation will be able to maintain an awareness of what personal data is being processed where within the system, and so will be unable to control or mitigate risks towards that data. Risk of duplicate or excessive data being processed. **Breach of Articles 5 (1) (c) and Article 30.**	All the processes in which personal data is used in the different phases of an AI system have been mapped out.	Data Index
			The mapping and then subsequent assessment for the potential minimisation of data includes data used in the production of the system and then as part of ongoing research to retrain the system	
			The personal data used in each phase of the AI system lifecycle has been indexed.	
			There is automated data tracing implemented to track the data being processed across the whole system	
			There is a process in place that detects any duplicated data present in different phases (from production to research) and deletes where necessary.	
4. There is a documented retention policy / schedule in place and	**<u>Buyer</u>** - to ensure that the buyer has control over the retention of personal	Without documented, monitored and adhered to schedules for retention,	There is a retention schedule based on business need with reference to statutory requirements and other principles	Retention Schedule Destruction Schedule, Log and / or Certificates

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).	data and is not bound by the decisions of the software developers. **Builder** - to review retention policies or schedules implemented by end users, in order to ensure that the system is built to allow the organisation using the it to determine appropriate retention periods.	there is a risk that personal data will be retained for longer then necessary, become inaccurate and excessive for the purposes for which it was collected. **Non compliance with Article 5 (1),(c).**	The schedule provides sufficient information for all records to be identified and disposal decisions put into effect.	
			Weeding activities are standardised, documented and occur on an ongoing or regular basis e.g. a process of rolling deletion of data.	
			The retention schedule is regularly reviewed to make sure it continues to meet business and statutory requirements	
			Where a review finds that the retention schedule is no longer adequate, this is remedied in a timely fashion	
			Responsibility for retention and disposal is designated to an appropriate person (this could be centrally or in each department e.g. IAOs)	
			All personal data held within AI systems are deleted / destroyed in line with the Retention Schedule	
			Where it is not possible to permanently delete the data (due to system functionality restrictions), data is stored securely 'out of reach' and access is locked down, or anonymised.	
			There is evidence that training data that is no longer required is removed or erased (e.g., because it is out of date and no longer predictively useful).	
			Where a decision has been taken to keep personal data outside the retention period, the justification for this has been documented and approved.	
			There has been a consideration of reproduceability - being able to reproduce the results at a later time, but unable to do so as the original data from the time has been deleted.	
			There is evidence of management sign off/approval prior to the disposal of personal data	
			Any failure to destroy personal data in line with the Retention Schedule is reported as an incident and dealt with accordingly	
			There is evidence to confirm that non-required features or data are removed or deleted	

Control	Control Objective	Risk	Indicators	Suggested Evidences or Documentation
1. There is evidence of a policy / process for dealing with individual rights (IR) requests in the data processing pipeline	To ensure there is a documented process for dealing with individual rights requests (e.g. IR requests relating to data used to train versus data produced as part of the output of the AI system)	Without a documented process which considers data within the processing pipeline and how IR requests would be handled during this time there is a risk that the UKGDPR would be breached and the rights of individual's ignored. Non compliance with Article 12-22.	There is a policy / process in place that defines how individual rights requests will be dealt with and by whom.	Individual Rights Request (IRR) Policy
			There is a specific person or team responsible for managing and responding to requests	Individual Rights (IR) handling procedures
2. There is documented guidance available for data subjects on how to make a request.	To ensure that end users are properly informed of what their rights are and how to invoke them. To ensure that individuals are not prohibited from exercising their rights in certain mediums, such as verbally.	Without clear guidance, data subjects may be unaware of how to, or simply be unable to, effectively invoke their rights. **Non compliance with Article 12-22.**	Information or guidance is included within privacy information to inform individuals how to make a request	IR training material for all staff (on how to recognise a request and where to channel requests)
			Information includes the name of the DPO	Job descriptions for roles with responsibilities for processing IRR's
			Individuals are given various ways or options in which to submit a request	IR web page/privacy policy
3. 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.	To ensure the builder has included functionality to allow the buyer to maintain an awareness of what personal data is being processed where within the system, to ensure that IR requests can be actioned within statutory timescales	Without appropriate data indexing / tracing systems and searchable functionality within AI systems there is a risk that statutory timescales will not be met, breaching Article 15 of the UKGDPR.	DPIAs include a consideration of how requests can be managed as part of the system design	Request form and any associated guidance for requestors
			There is a data indexing system in place to easily locate relevant data should a request be received	IR clauses within processor contracts
			Key 'search' words / common identifiers have been build into the system design	Template letters for clarification of request / request for more information
			Consideration has been given to whether responses can be automated within the system	Template letters for acknowledgement of request
4. The organisation systematically monitors the time taken to respond to requests in order to identify systems which are potentially more complex.	**Buyer** - To ensure that the organisation is able to identify opportunities to improve their performance, and is able to demonstrate a commitment to doing so. **Builder** -To ensure that the organisation has built in the ability to monitor the performance in response to requests, where possible, in order to facilitate performance management.	If there is no monitoring of performance, the organisation cannot act effectively to improve their performance. They may also be unable to effectively demonstrate their compliance with statutory requirements. **May breach Article 5 (2).**	There is a log of all requests (both verbal requests and requests in writing)	Template letter(s) for delays and extensions to response timeframes
			Dummy' IR requests are submitted to test the process, and measure the outcomes.	IRR Log
			There is management information gathered and reported to senior management showing the number of requests received and the percentages completed within statutory timescales	File / records / data retrieval procedures
			KPIs are in place to track performance	Details of redaction software/methods used
			There is a process to collate information on issues and trends causing delays in responding to requests	Data Index
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	**Buyer** - To ensure that the organisation using the AI system has embedded some form of effective logging and reviewing of purely automated decisions in their processes. **Builder** - To ensure that the organisation	If requests are not properly logged, reviewed, or actioned, then the organisation will run the risk that decisions may be made regarding data subjects which breach their rights under Article 22. **Non compliance with Article 22.**	There is a log of all requests received	IRRs performance dashboard - showing
			There is evidence that the decision made by the AI has been reviewed and an assessment undertaken to determine whether other individuals could have been impacted by any inaccuracies. The decision is changed where necessary.	Cold case review schedule.
			Individuals are given the means to provide additional data in order to be identified within AI systems or decisions reviewed.	Covering letters explaining reasons for withholding information

	which developed the AI system built into the functionality to allow for effective logging and reviewing of purely automated decisions.		Any inaccurate personal data and contextualises inferred data is corrected so that it is not misleading as to a matter of fact.	Template letters where individual is informed of their right of appeal or complaint
			There are procedures in place for customers to access the personal data input into the profiles so they can review and edit for any accuracy issues	Records of complaints received
			There are additional checks in place for profiling/automated decision-making systems to protect any vulnerable groups (including children).	
			There are written procedures / guidance in place to provide a simple way for individuals to ask for a reconsideration of an automated decision. Reviews and change decisions are only actioned by authorised staff.	
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 AI system(s).	The organisation has appropriate methods in place to erase, suppress or otherwise cease processing personal data without undue delay and within one month of receipt (unless an extension applies).	Without appropriate processes in place there is a risk that data will continue to be processed against the wishes of an individual, and that individual's IR will be breached. **Non compliance with Article 21.**	There are appropriate methods in place to erase, suppress or otherwise cease processing personal data without undue delay and within one month of receipt	
			Where a request is refused, relevant information is provided to the requestor in a timely manner (with the reasons for refusal clearly outlined).	
			All requests (verbal and written) are logged and the log is updated io monitor progress as each request is processed. The log shows the due date for requests, the actual date of the final response and a brief explanation for the reason for any refused requests.	
			There are procedures in place to inform any recipients (data processors) of all objections to processing and the data controller seeks confirmation from the processor that processing has ceased.	
			There is an accurate and up to date list of all data subjects that have objected to the processing of their data e.g. suppression lists for direct marketing	
			Performance in handling requests is monitored and that intelligence is used to improve performance and procedures.	
			There is clear information in privacy notices about individuals' right to object, which is presented separately from other information on their rights.	
			Peer reviews are conducted to ensure all actions have been completed as required.	
7. 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).	The organisation has appropriate methods in place to erase, suppress or otherwise cease processing personal data without undue delay and within one month of receipt (unless an extension applies).	Without appropriate processes in place there is a risk that data will continue to be processed against the wishes of an individual, and that individual's IR will be breached. **Non compliance with Article 17.**	There are processes in place to ensure that requests are responded to and actioned without undue delay and within one month of receipt (unless an	
			Where a request is refused, the relevant information is provided to the requestor in a timely manner (with the reasons for refusal clearly outlined).	
			If the request relates to data collected from children, there are specific procedures in place to deal with any request for erasure – especially any processing of their personal data on the internet.	
			All requests (verbal and written) are logged and the log is updated to monitor progress as each request is processed. The log shows the due date for requests, the actual date of the final response and a brief explanation for the reason for any refused requests.	
			There are procedures in place to inform any recipients (data processors) if data has been erased. This should include personal data that has been made public in an online environment.	
			Performance in handling requests is monitored and that intelligence is used to improve performance and procedures.	
			Peer reviews are conducted to ensure all actions have been completed as required.	

Control measures	Evidences			Assurance	Report Text					QA
	Documentation	Interview	Testing	Rating	Findings	Non Conformities	Recommendations	Priority	Best Practice	QA Comments
Contracts & 3rd Parties										
1. There has been a full consideration of the controller/processor/ joint controller relationship throughout the whole supply chain in the use of AI systems				Green	hbgivboiu	nfvo inbwfp iowbnf	dvbn owb ow	Urgent		
2. The decision reached on the controller / processor relationship across all proposed processing activities is documented.										
3. 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.										
4. Where the use of an AI system results in the creation and therefore processing of new attributable personal or special category data, due diligence checks are undertaken to ensure that individuals have either already received appropriate privacy information or else are provided with it in a timely manner.										
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 AI systems.										
6. There is an appropriate level of due diligence undertaken prior to any arrangement being agreed to ensure that appropriate measures will be in place to protect and enable individual rights										
7. When procuring AI systems or services, there is evidence that the buyer has considered what their acceptable level of system output accuracy is and has completed due diligence to ensure the product meets these accuracy requirements.										
8. 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).										
9. 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.										
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.										
11. Contracts are managed and reviewed										
12. Written contracts include all the 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										
14. PROCESSOR ONLY: 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.										
15. PROCESSOR ONLY: 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.				Green						
Data minimisation										
1. 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.				Yellow						
2. There is ongoing monitoring and testing of data use to ensure only the minimum data required is being processed by the AI system.										
3. 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.										
4. 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).				Green						
Individual Rights										
1. There is evidence of a policy / process for dealing with individual rights (IR) requests in the data processing pipeline				Yellow						
2. There is documented guidance available for data subjects on how to make a request.										
3. 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.										
4. The organisation systematically monitors the time taken to respond to requests in order to identify systems which are potentially more complex.										
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										
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 AI system(s).										
7. 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).				Red				Urgent		

Control	Control Objective	Risk	Indicators	Suggested Evidences or Documentation
1. BUILDER: All key roles in the design, development and testing of AI systems have received appropriate training in data protection and information security.	Ensuring that specialised technical based roles receive appropriate data protection / privacy training so that they have an appreciation for privacy by design principles and information risks. This training should be specific to the responsibilities of the individual, and subject to refresher training on a regular basis.	If technical staff and system designers do not understand privacy by design principles and potential privacy risks, then they may not consider these factors when designing the AI system. Breaches caused by lack of specialist knowledge. **Non conformance with GDPR Article 5 (1) & (2).**	Training needs analysis has been completed for all key roles involved in the design, development, approval, implementation and testing phases of an AI Human reviewers have received appropriate privacy training Training / Skills requirements are detailed in role job descriptions There is evidence to confirm up to date and appropriate specialised training has been completed by key roles AI system developers are retrained following issues with the system	Data protection and security training materials, e-learning
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.	Ensuring that privacy roles receive additional technical training to allow them to have some basc understanding of the technical nuances of an AI system in order to be able to fully assess the privacy implications of decisions made (e.g. through the DPIA). This training should be specific to the responsibilities of the individual, and subject to refresher training on a regular basis.	If staff within privacy / data protection roles do not have the technical expertise to understand the basics of the system design and the technical specifications or jargon, then they may not be able to fully assess the privacy implications of the design or provide a consultation service for any risk assessment. Breaches caused by lack of specialist knowledge. **Non conformance with GDPR Article 5 (1) & (2).**	There is an overarching technical training programme in place for privacy, Training needs analysis has been completed for all key postholders Training / Skills requirements are detailed in role job descriptions There is evidence to confirm up to date and appropriate technical training has been completed by key postholders Training is refreshed and redelivered following issues with the system	Training Programmes Training Needs Analysis
3. 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.	To ensure that when considering the requirements for each role, there has been an assessment of the skills and knowledge required from all applicants and that those recruited to the role can evidence the required qualifications.	If the organisation does not assess the skills, knowledge and qualifications that would be a pre requisit for each applicant applying for a role, then they may recruit someone who is not adequate for the role in question.	Job descriptions / adverts include a minimum set of competencies, skills and qualifications required for each post Recruitment processes include appropriate assessments to determine a candidates suitability for the role advertised Candidates that are 'self taught' are not excluded, however there are reasonable checks in place as part of the recruitment process to ensure they do retain the right level of knowledge and understanding for the role.	Job decsriptions Recruitment / Job Adverts Recruitment procedure / policy
4. Staff within both technical and privacy roles continually develop and maintain up to date skills and knowledge to enable them to effectively fulfil their responsibilities in their role(s).	As new technologies and processes in the AI sphere can develop and evolve rapidly, privacy and technical staff should keep their skills and knowledge up to date through various means, such as attending forums or focus groups, undertaking new training regularly, completing new qualifications etc.	If staff with technical or privacy roles do not refresh or update their skills and knowledge on a regular basis they may not be up to date on the latest technologies, advancements, privacy issues or risks, impacting the effectiveness and lawfulness of their AI system or service.	There is a programme of ongoing training needs analysis in place for key roles There is evidence that the organisation actively seeks out new training opportunities for key staff Staff in technical and privacy roles are supported in the completion of external qualifications to enhance their skills / knowledge Staff in technical and privacy roles have completed appropriate external training courses on a regular basis to update their knowledge and skills Staff in technical and privacy roles are attend Forums, Conferences, joint working groups etc in order to share and update knowledge / skills across various organisations or sectors Staff have read or themselves published research and academic papers Staff in technical and privacy roles have enrolled in various publications / newsletters, online groups or chats, book clubs etc in order to keep up to date on the latest technical and privacy news.	

5. Training has been provided to individuals involved in the assessment of lawful bases.	To ensure that individual's making the assessment understand the lawful bases, their implications on individual rights and how they may affect the potential lawfulness of proposed processing activities.	Incorrect lawful bases may be applied which risks that the processing may be unlawful under the GDPR. **Non compliance with Article 6 & 9.**	There is evidence to support that key staff have received additional training in the assessment of lawful bases	
			Training content is accurate, up to date and reviewed periodically	
6. All functions and individuals responsible for the development, testing, deployment and monitoring of AI systems are adequately qualified to understand the associated statistical accuracy requirements and measures	To ensure that key personnel involved in the process are appropriately skilled through training	Without appropriate training, key personnel could make errors when assessing the statistical accuracy of the system.	There is evidence to support that key staff (including human reviewers) have received training or have an appropriate qualification to understand the associated statistical accuracy requirements and measures	
			Training content / qualification is accurate, up to date and reviewed and / or refreshed periodically to ensure staff stay up to date with the latest technical advancements in the field	
7. There is evidence that AI developers and human reviewers are adequately qualified to identify and address bias and discrimination in AI systems.	To ensure key personnel are appropriately skilled and trained to identify bias or discrimination in the system effectively.	Without appropriate training key personnel may miss potential or actual bias or discrimination within the AI system	There is evidence to support that key staff have received training or have an appropriate qualification so they can identify and address bias and discrimination in AI systems	
			Training content is accurate, up to date and reviewed and / or refreshed periodically to ensure staff stay up to date with the latest technical advancements in the field	
8. AI systems developers receive training and have access to guidance on the requirement to consider individual rights (IR) at the offset.	To ensure that key personnel involved in the process are appropriately skilled through training	Without appropriate training, key personnel may not be aware, understand or have considered the impact to an individuals rights when developing the system. **Non compliance with Article 12-22.**	There is evidence to support that systems developers have received additional training to understand individuals rights under data protection law and recognise the impacts to these of AI systems.	Individual Rights policies Product management / release processes
			Guidance is available for reference on an ongoing basis	
			Training content is accurate, up to date and reviewed periodically	
9. Customer facing staff receive training on Chapter 3 of the UK GDPR on individual rights, and there are appropriate SOPs / procedures in place. The training or procedures include how to escalate more complex requests.	To ensure that key personnel involved in the process are appropriately skilled through training	Without appropriate training for 'customer facing' staff, there is a risk that IR requests will not be recognised, channelled to the right staff to action or escalated as necessary, **breaching Article 15 of the GDPR**	There is documented guidance available to staff on how to recognise a request, covering both verbal requests and requests in writing	
			There is documented guidance available to staff on how to appropriately channel a request	
10. BUYER: 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 prior to and during the use of the AI system their organisation has purchased.	Ensuring that privacy roles receive additional technical training to allow them to have some basc understanding of the technical nuances of an AI system in order to be able to fully assess the privacy implications of decisions made (e.g. through the DPIA). This training should be specific to the responsibilities of the individual, and subject to refresher training on a regular basis.	Breaches caused by lack of specialist knowledge. **Non conformance with GDPR Article 5 (2).**	The developer provides training to its buyers/users to ensure that they use the system in the way it was designed so that they interpret the results as	
			Training is delivered prior to the purchase of the system to allow the buyer to conduct a thorough DPIA	
			Training is provided following each change, reconfiguration or patch of the	
			There is an overarching technical training programme in place for privacy, risk and audit staff.	
			Training needs analysis has been completed for all key postholders	
			Training / Skills requirements are detailed in role job descriptions	
			There is evidence to confirm up to date and appropriate technical training has been completed by key postholders	
			Training is refreshed and redelivered following issues with the system	

Control	Control Objective	Risk	Indicators	Suggested Evidences or Documentation
1. 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.	To ensure that there is proactive engagement and communication between a buyer and builder and / or controller and processor to fully assess the privacy risks within the AI system / service, prior to the procurement of any AI service or system.	If builders and / or processors are not actively engaged in the risk assessment process conducted as part of the due diligence prior to procurement of an AI system or service, then there may be a gap in the risk assessment completed which could lead to a breach in the UK UKGDPR or a failure in operating effectiveness of the system and a detrimental impact on the business / service provided.	There are meeting notes or emails in place to demonstrate proactive discussions and engagement between all parties	Client product reports. Sales reports/ materials, technical documents. Template DPIA / model DPIA answers from builder. DPIA screening checklist DPIA template DPIA policy / procedure / process Technical specification document(s)
			The due diligence process includes a requirement to co-ordinate risk assessment activities across all parties	
			There is a screening checklist in place to aid in consideration of whether a DPIA is required.	
			The screening checklist includes all the relevant considerations on the scope, type and manner of the proposed processing.	
			Model DPIAs have been created that can be given to purchasers to use, rather than responding to individual requests.	
2. 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.	**Buyer** - The DPIA must clearly show the decision making around the purpose of the AI and its goals, and detail the data flows, processing and outputs expected from a purchased AI and the testing strategy to evaluate the system's performance. **Builder -** The DPIA must document the purpose of the intended AI build, detail how it is intended to function, the expected outcomes and evaluation and testing strategy.	If the DPIA does not provide sufficient detail around the purpose and functionality of the AI it may not be compliant with Article 35 of the UKGDPR.	DPIAs are reviewed for different stages of system development - research, training etc	Data flow map
			There has been a MoSCoW (must, should, could, would like to have) approach taken when determining the scope and functionality of the AI system and the various models deployed within the system	
			The DPIA includes a summary of what the AI system is intending to do, what processing this will involve and what the outputs are expected to be	
			DPIAs clearly set out the relationships and data flows between controllers, processors, data subjects and systems.	
			A data flow mapping exercise has been completed to document the data that flows in, around and out of an AI system	
			The process / template includes a check that the processing is necessary for and proportionate to the purposes.	
			The proposed system testing regime / plan (pre and post implementation) has been considered and documented within the DPIA	
3. There is a DPIA policy / process in place, with supporting templates and guidance to facilitate the completion of an effective DPIA that meets the requirements under the UKGDPR (Article 35)	The DPIA process is defined in a detailed policy and backed up with standard operating procedures, a template document and decisions making thresholds, with appropriate review and sign -off points and there is evidence that the policy and processes are themselves reviewed.	If the DPIA process is not well-documented, uniformly applied and kept under review there is a risk of non-compliance with Article 35 of the UKGDPR.	There are references to DPIA requirements in all main project and change management policies and procedures.	
			The procedures stipulate that a DPIA should begin early in the life of a project, before processing starts, and that the DPIA should run alongside the planning and development process.	
			There is a documented process / policy in place, with appropriate document controls, that is reviewed periodically to ensure it remains up to date.	
			The organisation has a standard DPIA template in place	

			There is a version of the DPIA which is structured and clearly documented, written in plain English, that can be understood by a non- specialist audience, as well as a more technical version.	
			Despite being written in a clear language, DPIAs still contain the necessary technical detail to describe the nature, scope, context	
			DPIAs identify measures that can put in place to eliminate or reduce high risks.	
			The process / template includes an objective assessment of the likelihood and severity of any risks to individuals’ rights and	
			The process / policy provides guidance for staff so they understand what a DPIA is and why it is necessary.	
			Responsibility for completing DPIAs is assigned to a member of staff who has sufficient control over the project to effect change e.g. Project Lead/Manager	
4. There is evidence that internal stakeholders, technical specialists within AI product teams and data subjects (or their nominated representative(s)) have been consulted as part of the DPIA assessment as appropriate.	To ensure that all relevant internal stakeholders, technical specialists and external data subjects have an opportunity to input on a DPIA, rather than it being filled out by a single person with potentially limited specialist knowledge.	If no internal or external consultation takes place, specialised areas of the DPIA may be completed by non specialists or individual rights / impacts on data subjects may not be considered and so risks may go unaccounted for. **Non compliance with Article 35.**	The process for completing a DPIA includes consultation with internal DP specialists (such as the DPO), internal technical specialists or equivalent and external data subjects (or their representatives).	User engagement for design of products, UAT on actual user experience.
			There is a process for seeking input and consultation from all relevant stakeholders which includes the requirement to document any decisions on how they determined which stakeholders to consult with (and why some were excluded if applicable).	
			Discussions and outcomes of all consultations are documented / recorded	
5. Appropriate senior management have oversight of completed DPIA reports and sign off on the outcome of the assessment.	To ensure that senior management have an awareness of the findings of the DPIA, to allow it to be effectively implemented.	If relevant staff do not receive visibility of the DPIA report, then there is a risk that a project will be implemented without agreed controls being put in place. **Non compliance with Article 35.**	The report is disseminated to appropriate stakeholders	
			There is a standard dissemination list for DPIAs	
			The organisation receives confirmation of receipt by those the report is disseminated to	
			The report is formally presented at a meeting of the Information Governance Board (or equivalent)	
6. The outputs of a DPIA are acted upon to effectively mitigate or manage any risks identified.	To ensure that personal data is not put at risk by being processed without risk assessment or controls.	If processing takes place prior to a DPIA, or before mitigating controls are put in place, then there is greatly increased risk that there may be a PDB as information is being processed without risk assessment or control. **Non compliance with Article 35.**	The DPIA policy requires that processing is not undertaken until the mitigating controls have been implemented	
			The project management policy (or equivalent) includes a stage of confirming that mitigating controls are now in place	
			The organisation retains evidence to confirm that processing was not begun until mitigating controls had been implemented	
			DPIAs are incorporated into the project plan/project risk register	
			Where the residual risk is high and cannot be further mitigated, there is a process to refer the DPIA to the ICO for review	
7. 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.	To ensure that changes to the context of the project or the organisation are accounted for as processing activities continue.	As projects go forwards, often they are adjusted or changed to fit new circumstances. If the DPIA is not reviewed periodically, new risks may emerge which are not identified and are left uncontrolled. **Non compliance with**	DPIAs are assigned a formal date of review	DPIA Log
			There is a process by which an early review may be carried out if there is a substantial change to the nature of, scope, context, or purposes of the process	
			There is evidence of regular reviews / meeting to discuss product performance and issues that links back to the DPIA	
8. There is an effective risk management	**Buyer** - To ensure there is a documented process	Without an effective risk management	There is an overarching risk management strategy in place	Risk management policy / procedure

strategy in place to facilitate the formal documentation of risks associated with the use of AI systems and ensure they are tracked and managed at a corporate level through an appropriate risk register	around managing and mitigating the risks involved in selecting, screening (due diligence) and deploying AI systems **Builder** - To ensure that personal data risks in the development of an AI are captured on a pre-existing registers, or if kept on a separate personal data risk register are also escalated to the corporate register where necessary.	strategy, the data controller will be unaware of the risks involved in this type of processing and be unable to mitigate them, threatening individuals rights and freedoms and risking a breach of the UKGDPR. Non conformance with UKGDPR Article 5 (2).	There has been an assessment of the level of risk and risk appetite which is dependent on the extent of the use of AI systems The data controller has used a recognised risk assessment framework to assess the risks involved with processing using an AI system Privacy risks are documented and tracked in a register Risks identified to statistical accuracy are logged and monitored through an appropriate risk register The risk assessment assesses the risks to individuals' rights that the use of AI poses and determines how to address these. The strategy includes an assessment of potential discriminatory effects on people based on their gender, race, age, health, religion, disability, sexual orientation or other characteristics. The organisation has appointed a senior member of staff with overall responsibility for risk management Risks have been documented for treat/transfer/tolerate/terminate (or equivalent) courses of action Appropriate action plans have been documented for all privacy risks that are designated to be treated or transferred Action Plans link into AI system development strategies / plans	Risk Register(s)
9. There is evidence that risks are being mitigated through ongoing AI system development / enhancements	**Buyer** - The user of the AI is maintains an evolving process of risk managing with a structured approach to allow them to track actions and respond to systems changes communicated by the vendor. **Builder** - To ensure that changes and enhancements required for systems are documented in action plans and managed effectively, and that system changes and enhancements are communicated to customers along with current mitigates and actions for them to consider.	Without an evolving and responsive risk management strategy there is a potential for static risk treatment. Non conformance with UKGDPR Article 5 (2).	Assurance is provided by developers on the progress against managing and mitigating the current risks associated with the system System changes, developments or enhancements planned as a result of the identification of privacy risks are fed back into the DPIA(s) or a new DPIA is initiated Appropriate action plans have been documented covering new or emerging risks as a result of system changes, developments or enhancements There are processes in place between buyer and builder to facilitate communication of new or emerging risks and discuss strategies or mitigations that can be deployed to address them. There are regular meetings or communications between the buyer / builder or controller / processor where ongoing risk management is discussed Risk registers reflect ongoing review of legacy, current or new risks and are updated by all parties as appropriate.	Change management process Change management log Client / supplier meeting minutes

Control	Control Objective	Risk	Indicators	Suggested Evidences or Documentation
1. There has been a thorough assessment of security risks to or in the AI system prior to its implementation to reduce the likelihood of an attack or breach	**Buyer -** To ensure that a full assessment is undertaken of the security risks to or in the AI system prior to its implementation as part of due diligence prior to purchase. **Builder -** To ensure there is a thorough assessment of security risk undertaken in the development and sales processes.	If a full assessment has not been undertaken there is a likelihood of an attack or breach. *Note fo r auditors. Mature IS/AI systems may use 'bug bounty' programs to identify vulnerabilities (Good Practice)*	The DPIA includes a thorough assessment of the security risks and the mitigants / controls to reduce the likelihood and impact of an attack or breach	DPIA
			Technical controls have been implemented to mitigate any security risks in the system design and build phases where appropriate.	
			Appropriately skilled technical experts have been consulted as part of the risk assessment e.g. traditional software engineers, systems administrators, data scientists, statisticians, as well as domain experts	
			An external security audit has taken place	
			Where existing systems need to be integrated, the impact on the security of the connected systems has been considered with appropriate controls put in place as part of the design and build phases.	
2. Security measures are in place to prevent privacy attacks on Machine Learning (ML) models through model inversion, membership inference or adversarial examples.	**Builder -** To ensure there are appropriate security measures in place to prevent privacy attacks on Machine Learning (ML) models through the personal data of the individuals whose data was used to train an AI system being inferred by simply observing the predictions the system returns in response to new inputs, for example by model inversion or membership inference. To ensure there are measures in place to prevent examples being fed into the ML model which have been deliberately modified so that they are reliably misclassified.	In a model inversion attack, if attackers already have access to some personal data belonging to specific individuals included the training data, there is a risk they can infer further personal information about those same individuals by observing the inputs and outputs of the ML model. The information attackers can learn goes beyond generic inferences about individuals with similar characteristics. Membership inference does not go as far however there is a risk that malicious actors could deduce whether a given individual was present in the training data of a ML model.	For biometric data e.g. facial images, there has been a consideration as to the ease at which an attacker could probe the model and reconsruct the image. Consideration has been given as to whether it is necessary to provide 'confidence' information to the end user (as this could be used to exploit the system).	Model / system security policy System Operating Procedures
			There are checks in place on the system to identify possible attacks where a large series of inputs / data / queries are entered into the system by a single source with the aim of identifying or extracting personal data of individuals e.g. through monitoring queries from users through the API.	
			There are measures in place to prevent the unauthorised extraction of data from either the main system or training data sets	
			There are measures in place to reduce the number of queries that can be performed by a particular user in a given time limit (rate limiting).	
			Different measures have been applied for 'black' and 'white' box attacks. *Note: 'white' box attacks are where the attacker has complete access to the model itslef to inspect underlying code, whereas 'black' box attacks the attacker can only query the model and observe relationships between inputs and outputs.*	
			Measures have been implemented to ensure that ML models are not vulnerable to privacy attacks through 'overfitting' i.e. the model has been designed to pay too much attention to the details of the training data, remembering particular examples rather than just general patterns.	
			Access to the underlying code and properties of the system / model is restricted.	
			Access to the model or training data for third parties is closely monitored and on a 'need to know' basis.	
3. There is ongoing monitoring of the AI system for software vulnerabilities. Security fixes are applied where appropriate.	To ensure there is ongoing monitoring of the AI system for software vulnerabilities and where identified, they are fixed / patched where appropriate.	The infrastructure and architecture of AI systems increases the likelihood of unauthorized access, alteration or destruction of personal data.	Where changes to an organisation’s software stack (and possibly hardware) have been made, there is a review to determine if there are any new security risks	Penetration Test Plans & Reports Internal IT health check plans and reports Patch Management Policy Vulnerability Monitoring Policy
			Technical security controls are documented within System Operating Procedures (SyOpS)	
			The organisation subjects software to a security review where one or more individuals view and read parts of its source code. At least one of the reviewers must not be the author of the code.	
			The organisation has implemented appropriate system vulnerability monitoring / testing tools or software	
			System vulnerability monitoring is logged and proactive analysis is conducted on any anomalies actively / results	
			The organisation subscribes to security advisories to receive alerts of vulnerabilities.	
			There is a solid patching / updating process in place so that available security fixes are applied in a timely manner.	
4. 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).	To ensure that regular tests are undertaken on security measures deployed.	Without regular testing of all security measures deployed there is no assurance that they remain effective in the prevention of a security incident or breach.	Independent internal reviews of the information security management system are undertaken, including internal audits and internal IT health checks (ITHC)	IT Risk Register
			There are external technical compliance reviews of key systems, including vulnerability assessments, ITHC and penetration testing	
			Issues and risks identified as part of any internal or external testing are captured on an action plan and risk register (and mitigated or treated as appropriate)	
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.	To ensure there is a policy / process for the separation of the AI development environment from the rest of the IT network / infrastructure and that the separation has been adhered to / happened.	If the AI development is not undertaken in a separate environment from the main network, then there is a risk to the security and integrity of the main network.	The policy includes details on how the organisation intends to segregate the AI system whilst in development from main IT networks	Back Up Policy / procedure
			Separation plans are included in the system design documents	
			The organisation keeps the AI system in a suitably secure environment.	
			There is a backup of the AI system in case the main AI system becomes unavailable. The back up is kept in a separate location.	
6. The organisation has effective asset management processes in place to ensure a coordinated approach to the security of data within it's systems.	To ensure there are documented approaches outlining asset management suitable to the classification and type of asset. This should extend to all computer systems involved in AI development and	Without a documented approach, there is a risk to the security of information held within its information assets.	There is a Hardware and Software Management Policy in place.	Hardware and Software Management Policy Hardware and Software asset registers Hardware and Software Risk Management Policy Acceptable Use Policy and procedures
			The data controller can provide a comprehensive overview of the assets it owns and/or operates	

	operation - includes developer's devices, production environments, live systems, data sets and connecting networks and infrastructure.		There is an established and appropriate risk assessment methodology applied to the asset registers/inventories	
			There are documented rules for the acceptable use of hardware assets	
			There are documented rules for the acceptable use of software assets	
7. 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.	To ensure contracts include appropriate information security clauses and good practice is adopted, for example - supplier / builder actively monitors 3rd party use of system for security vulnerabilities on their behalf and feeds back issues - continuous monitoring of critical vendors.	Without defining the role and responsibilities of 3rd parties in terms of security of personal data in AI systems there is a risk of a breach of the UKGDPR and a security incident / breach.	Due diligence includes system security and data security checks / assessments	Security based due diligence checklists and reports Example supplier and client contracts Procurement policy and procedures
			Appropriate technical measures and controls have been included in supplier and processor contracts	
			Contracts document the roles and responsibilities for supplier / processor staff and they have been provided with appropriate information security training.	
			Contracts include clauses entitling the data controller to conduct periodic information security based compliance checks on suppliers / processors, and these checks are undertaken.	
			Information Security considerations are built into the procurement process	
8. There is evidence of a policy / processes for data breach reporting and escalation.	To ensure there is a documented policy in place for data breach reporting and escalation	Without a documented policy / process for the management and escalation of personal data breaches, there is a risk that breaches will not be identified, logged, managed and mitigated effectively	Responsibility for managing breaches has been allocated to a dedicated person or team.	Breach Management Policy and procedures Breach Log Personal Data Breach training for all staff
			There are processes and systems in place to facilitate the reporting of personal data breaches	
			Both actual breaches and near misses are centrally logged / recorded / documented (even if they do not need to be reported to the ICO or individuals).	
			Analysis is undertaken on all breach reports to prevent a reoccurrence of the incident.	
			There is appropriate training in place to ensure staff recognise a personal data breach	
9. The organisation monitors systems/network activity to detect suspicious requests and **take action as a result**.	To ensure there is active / proactive monitoring of suspicious activity across network and computer systems and where detected is appropriate and effective measures are taken (blocking, alerts, system shutdowns)	Without active monitoring and resulting action, suspicious requests or activity could be missed which could threaten the functioning of the system and its effectiveness	There is evidence to confirm active monitoring of API requests takes place	System monitoring policy / procedures API Access Policy Firewall rules
			There is a log of all issues detected and issues are investigated and (where necessary) escalated	
			Action plans are in place to resolve issues identified	
			There is an API access policy in place which includes the process adopted to monitor volumes and patterns of API requests for suspicious activity	
			There are external and internal firewalls and intrusion detection systems in place as appropriate to ensure the security of information in networks and systems from unauthorised access or attack e.g. denial of service attacks	
			Network traffic is monitored for unusual or malicious incoming or outgoing activity	
			The organisation maintains an awareness of possible threats and acts swiftly to implement corrective measures	
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.	To ensure that the personal data collected by the organisation is not inaccurate, and also to ensure that no security threats are created through the collection of personal data. Ensure there are no routes to poison data, that incoming data is validated (e.g. when using web forms) and that encryption is used in data transfers.	If the organisation does not ensure the accuracy of the data collected, then it cannot rely on the outputs of the AI system to be accurate or useful. If effective security is not in place, data collection avenues may become a site of attack and result in a security breach. May breach Articles 5 (1) (d) and (f).	Data is encrypted across networks where required.	Data accuracy and integrity test plans Data Quality / Quality Assurance Policy and procedures
			Data in storage (at rest) is encrypted in line with risk e.g. SCD.	
			Measures are in place to secure data collection sites or web forms from malicious attacks or corruption (or DOS attacks)	
			Data accuracy and integrity testing is done on data sourced or collected from external sources or individuals	
			Data accuracy and integrity testing is done on data sourced or collected indirectly from third parties as part of the build and testing phases of the system development	
11. The organisation has in place effective mechanisms in order to prevent unauthorised access (read/write), or inappropriate changes being made to data sets.	To ensure that any personal data stored by the organisation is kept safe from inappropriate changes due to either internal and external attacks/actions/errors through user access management controls and detection/prevention mechanisms	If unauthorised or inappropriate changes are made to personal data the organisation risks the effectiveness of the outputs of their AI system being impacted. May breach Articles 5 (1) (a) and (d).	Access to the AI system is only provided where there is a legitimate need. Access is kept to the minimum necessary.	Access Control Policy Starter, Mover and Leaver Process Client system access process Role based access level 'lists'
			Access to personal information is limited to authorised personnel only.	
			A formal user access provisioning process has been implemented to assign access rights to staff	
			The allocation and use of privileged access rights is restricted and controlled.	
			User access rights are reviewed at regular intervals	
			Access rights are restricted or removed in a timely fashion for all staff	
			Access rights are adjusted upon a change of assignment/role	
			Users are made accountable for safeguarding their authentication information	
12. The organisation has in place effective mechanisms in order to monitor and track all changes being made to personal data.	To ensure that the organisation is aware of what changes have been made to personal data, who by, and when, in case there are any problems caused or complaints raised as a result of the	If changes are not tracked, then the orgnaisation cannot effectively investigate who is responsible for any inappropriate changes and may fail to detect a security	The organisation has processes in place to review the latest privacy enhancing techniques, assesses the technique's applicability to their context, and implement it where appropriate.	Logging Policy (to track changes to personal data in the system) Example event logs as a result of system monitoring activities
			Logging and monitoring is in place to record events and generate evidence.	

Appropriate background checks are carried out on personnel (employees,

	change. with independent or cold case reviews of changes to data records	breach. May breach Articles 5 (1) (d) and (f).	Event logs recording user activities and information security events are produced	
			Logs are subject to regular review	
			There is a documented Logging Policy	
13. There are business continuity and disaster recovery plans in place.	he extent to which the organisation has measures in place to ensure that personal data and data subjects are not adversely affected in the event of significant functional impacts on the organisation	Failure to effectively implement business continuity and disaster recovery may result in loss of access to personal data and the risk that personal data may not be processed in compliance with the regulations resulting in regulatory action and/or reputational damage. **Article 5(1)(f)**	The organisation has allocated responsibility for assessing, managing and reporting on Business Continuity (BC) and Disaster Recovery (DC) risks in a structured hierarchy.	Business Continuity Plans (BCP) Disaster Recovery Plans (DR) BCP & DR test reports / results
			The organisation has taken pro-active steps to identify, record and manage risks to BC and DC.	
			The organisation has put measures in place to safeguard against physical and environmental disruption.	
			The IT Change Management Process feeds into the organisation's BC and DR function.	
			The organisation has determined its requirements for Information Security (IS) and IS management in the event of a disaster, i.e. information continues to remain secure, by default if necessary.	
			The organisation has put in place a documented BC/DR policy and attendant procedures in place to manage high impact incidents.	
			The organisation has a documented Disaster Recover Plan (DRP) and attendant procedures in place to manage high impact incidents.	
			The organisation has included general BC/DR awareness and escalation training within the DP training programme.	
			Specialised training is in place for the Incident/Emergency Response team(s).	
			The organisation has put in place provisions for a temporary physical space in the event of loss of access to the primary site.	
			The organisation has a pre-determined restoration strategy in place appropriate to the importance of the system/data.	
			Key systems, applications, and data are backed up to protect against loss of personal data.	
			BC and DR arrangements have been built into all third party relationships.	
			BC/DR level events and near misses and their resolutions are analysed, reported and form part of the organisational learning strategy.	

Control measures	Evidences			Assurance	Report Text					QA
	Documentation	Interview	Testing	Rating	Findings	Non Conformities	Recommendations	Priority	Best Practice	QA Comments
Staff Training										
1. BUILDER: All key roles in the design, development and testing of AI systems have received appropriate training in data protection and information security.				Green	hbgivboiu	nfvo inbwfp iowbnf	dvbn owb ow	Urgent		
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.										
3. 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.										
4. Staff within both technical and privacy roles continually develop and maintain up to date skills and knowledge to enable them to effectively fulfil their responsibilities in their role(s).										
5. Training has been provided to individuals involved in the assessment of lawful bases.										
6. All functions and individuals responsible for the development, testing, deployment and monitoring of AI systems are adequately qualified to understand the associated statistical accuracy requirements and measures										
7. There is evidence that AI developers and human reviewers are adequately qualified to identify and address bias and discrimination in AI systems.										
8. AI systems developers receive training and have access to guidance on the requirement to consider individual rights (IR) at the offset.										
9. Customer facing staff receive training on Chapter 3 of the UK GDPR on individual rights, and there are appropriate SOPs / procedures in place. The training or procedures include how to escalate more complex requests.										
10. BUYER: 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 prior to and during the use of the AI system their organisation has purchased.				Green						
DP Risk Management										
1. 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.				Yellow						
2. 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.										
3. There is a DPIA policy / process in place, with supporting templates and guidance to facilitate the completion of an effective DPIA that meets the requirements under the UKGDPR (Article 35)										
4. There is evidence that internal stakeholders, technical specialists within AI product teams and data subjects (or their nominated representative(s)) have been consulted as part of the DPIA assessment as appropriate.										
5. Appropriate senior management have oversight of completed DPIA reports and sign off on the outcome of the assessment.										
6. The outputs of a DPIA are acted upon to effectively mitigate or manage any risks identified.										
7. 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.										
8. There is an effective risk management strategy in place to facilitate the formal documentation of risks associated with the use of AI systems and ensure they are tracked and managed at a corporate level through an appropriate risk register										
9. There is evidence that risks are being mitigated through ongoing AI system development / enhancements				Green						
Security & Integrity										
1. There has been a thorough assessment of security risks to or in the AI system prior to its implementation to reduce the likelihood of an attack or breach				Yellow						
2. Security measures are in place to prevent privacy attacks on Machine Learning (ML) models through model inversion, membership inference or adversarial examples.										
3. There is ongoing monitoring of the AI system for software vulnerabilities. Security fixes are applied where appropriate.										
4. 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).										
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.										
6. The organisation has effective asset management processes in place to ensure a coordinated approach to the security of data within it's systems.										
7. 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.										
8. There is evidence of a policy / processes for data breach reporting and escalation.										
9. The organisation monitors systems/network activity to detect suspicious requests and **take action as a result**.										
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.										
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 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.				Red				Urgent		

Control	Control Objective	Risk	Indicators	Suggested Evidences or Documentation
1. 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.	**Buyer** - Has considered potential trade-off decisions when selecting an AI system, for example individual privacy vs the goal of the AI output. Less privacy intrusive approaches have been considered. **Builder** - Has undertaken a 'trade off analysis' and considered potential trade-off decisions when building an AI system, for example balancing individual privacy against the use of PID in testing	Inadequate or inappropriate trade-off analysis / decisions lead to AI systems that incorrectly prioritise one criterion over another more important criteria. Potential **non conformance with Article 5(1)(a) or (b), Article 25 (potential to be in breach however of any principle here).**	The methodology for identifying and assessing the trade-offs in scope; the reasons for adopting or rejecting particular technical *Where appropriate:* There is analysis done which includes consideration as to whether a trade off between the accuracy of the algorithm (s) used is too complex to work with by those involved in the processing and to be explained in privacy information vs. a lower level of accuracy but it being understood by those involved in the processing and can be accurately explained in privacy information. There has been a consideration of available technical approaches to minimise the need for any trade-offs	Product release documentation Experiment Logs Meeting reports / briefings Training reports iBeta testing & certification - good practice?
2. Decisions made during the trade off analysis have been documented and signed off at an appropriately senior or expert level.	**Buyer** - The decision to purchase or use the AI system following the trade off analysis are documented and signed off at appropriately senior or expert level. **Builder** - Decisions over the use of personal data within and by an AI have been made and signed off by staff at appropriately senior and/or experience level. Less privacy intrusive approaches have been considered.	Without full consideration and documentation of the decisions made for all potential trade offs, and subsequent appropriate approval, there is a risk that systems will be developed that are unsuitable or pose a risk to personal data or an individuals privacy. **Potential non conformance with Article 5(1)(a) and 5 (2).**	The organisation has reviewed the trade-off options and provided justification as to why the specific model / system was selected e.g. There are clearly documented criteria and lines of accountability about the final trade-off decisions The specification has been signed off by appropriate management.	Documented trade off decisions
3. As part of model and system 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).	As part of model and system development, there could initially be more human work and review needed to ensure functionaility and accuracy, however over time this work will become more automated as the AI develops. To ensure there has been a careful consideration of the trade off between the level of human work and automation with only human review. Documented record of the decision to move to more automation and the impact on accuracy this could have.	If the organisation does not carefully consider the move towards automation, and the trade off this could have on accuracy, there is a risk the system will not be ready for full automation and will start to produce inaccurate results. Article 5(1)(a)-(f)	The product / technical specification documents include a development timeline with set milestone / review dates Each move to further automation os tested for accuracy and signed off	
4. 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.	**Buyer -** To ensure that trade-offs are kept under review as the AI generates output over time as new considerations and competing priorities may emerge. **Builder -** To ensure that changing or potentially new trade- offs are considered and documented during the development process, particularly where new data sets may require the development of a new product. To ensure trade off analysis is linked to and included in the overall change management process.	Without maintaining a continuous review of the system, there is a risk that new emerging trade offs will not be considered or approved. **Potential non conformance with Article 5(1)(a)-(f) and 5 (2).**	The organisation periodically re-analyses trade-offs for new data created due to the ongoing function of the AI system. Changes are approved, documented and communicated to individuals and staff. If new data sets become available, a new product is released rather than add this new data to an existing system / model if there is the potential for this to impact on system performance, bias, discrimination, statistical accuracy etc.	

Control	Control Objective	Risk	Indicators	Suggested Evidences or Documentation
1. The organisation has methods in place to ensure that the data sets relied on for determining statistical accuracy are accurately and fairly labelled.	To ensure that the builder's determination of statistical accuracy has a solid foundation and is not relying on inaccurately labelled data. And further, to ensure that the labels used when labelling the data are fair on the data subjects, particularly that they are within the bounds of what the data subject may reasonably expect to be labelled as, and that the labels used will not cause outcomes which may have an unreasonable impact on the data subjects. Decisions made regarding features that won't be labelled have been documented.	If data sets are not accurately labelled, then any statistical accuracy derived from those data sets cannot be relied upon. This may result in processing activities which are unfair on the data subject. **Non conformance with Article 5(1)(a).** For systems covered by the AADC, also consider whether the labelling is fair under the expectations of the Code.	There are data management processes in place and documented that detail the data labelling requirements and steps. The requirements should be easy to understand, include descriptions of all possible labels, examples of every label, and cover edge cases.	Data management process Data labelling process Data labelling QA process Data labelling testing results Contracts for 3rd party data labelling services Evidence of data label reviews
			Staff responsible for determining the labelling of data sets are appropriately skilled, qualified, knowledgeable and diverse to ensure the quality and accuracy of labels set	
			The labelled data used to train the AI is based on a statistically representative sample so as not to bias the results	
			The labelling process includes QA procedures which covers both subjective (where there is no single 'correct' label for the data and so the label is assigned subjectively by the labeller) and objective (where there is a 'correct' label, but the labeller may not know how to apply it to the data in question e.g. a car can be labelled as a single entity, or the parts of a car can be labelled individually).	
			Labelling is analysed for blind spots and biases	
			Testing of labelling includes an analysis of 'edge cases' (rare and unusual situations which do not happen often) to ensure these are not excluded / missed or misinterpreted.	
			Data is added incrementally into the data labelled sets to increase the accuracy of the systen with the least amount of data	
			For automated labelling, there are 'human in the loop' based QA processes in place as part of the labelling process	
			Where a 3rd party data labelling service is used, all the principles of the UKGDPR are applied in practice e.g. security	
			There has been a consideration of research, academic papers, sector requirements to determine data labels, which could include consultation with members of protected groups or their representatives to define the labelling criteria.	
			There is a process to ensure that where disagreements on labelling for edge cases occurs, an independent 'third person' will be consulted.	
			Decisions made regarding features that won't be labelled have been documented.	
			Data labels are kept under review.	
2. There is pre-implementation statistical accuracy testing of new AI 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	**Buyer -** To ensure the statistical accuracy of a purchased system is adequately tested with output documented along with refinement decisions. **Builder -** To ensure that components and integrated systems have been tested for statistical accuracy prior to deployment, according to a documented test plan.	Without a structured testing process in place there is a risk that pre implementation testing will not be undertaken or completed effectively. If pre implementation testing does not occur, issues with statistical accuracy may not be picked up in a	There is a policy / documented process in place that includes details of how the system will be tested prior to implementation	Statistical accuracy test plans Statistical accuracy test results , charts etc.
			The 'test plan' includes all the relevant checks to ensure that there are no errors in data outputs or statistical errors.	
			The test plan includes documented tolerances for errors	

organisation's required statistical accuracy level has been achieved.		timely manner and inaccurate or biased system outputs may occur. **Non conformance Article 5(1)(a).** By not documenting the outcomes of such testing there is no audit trail.	The test plan includes minimum success criteria, set as a % baseline acceptable for current performance - false acceptance and rejection rates are monitored. The results of the testing are documented Acceptance of the test results are signed off by management There is evidence to confirm that the AI system has been 'retrained' following testing (e.g. by improving input data, different balance of false positives and negatives, or using different learning algorithms) The organisation tests the AI system on new data set(s) to confirm the same outcome is reached. There is evidence that testing was completed prior to the deployment of the AI system.	
3. 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.	**Buyer -** To ensure structured, periodic, human reviews of output, pre and post-deployment where possible to independently validate the statistical accuracy of the purchased system **Builder -** To ensure that human reviews are conducted where possible on AI decisions to independently test statistical accuracy using a pre-defined process, varying the inputs and re-evaluating as the system is retuned.	Without a structured testing process in place there is a risk that a human review will not be undertaken or completed effectively to provide an independent assessment of AI system outputs. **Non conformance Article 5(1)(a).**	There is a policy / documented process in place that includes details of the methodology that will be used by a human There is a testing process in place that outlines the test plan criteria, requirements and sampling method / size. The 'test plan' includes all the relevant checks to ensure that the rate of error in data outputs or statistical errors is within acceptable and documented tolerances. The test plan includes documented tolerances for errors The results of the testing are documented Acceptance of the test results are signed off by management There is evidence to confirm that the AI system has been 'retrained' following testing (e.g. by improving input data, different balance of false positives and negatives, or using different learning algorithms) The organisation tests the AI system on new data set(s) to confirm the same outcome is reached.	Product Performance dashboards
4. Post-implementation testing is carried out and the results of the testing and action(s) taken as a result are documented.	**Buyer** - To ensure the organisation has a pre-defined testing process to assess AI functionality and output after deployment, including communication with the developer to ensure assumptions are correct and necessary refinement can take place. **Builder** - To ensure communications channels are maintained and the developer supports post-implementation testing in a documented and collaborative way.	Without a structured testing process in place there is a risk that post implementation testing will not be undertaken or completed effectively. **Non conformance Article 5(1)(a).** If results of testing are not documented there is no effective audit trail.	There is a policy / documented process in place that includes The test plan includes all the relevant checks to identify any errors in data outputs. The test plan includes documented tolerances for errors The results of the testing are documented Acceptance of the test results are signed off by management There is evidence to confirm that the AI system has been 'retrained' following testing (e.g. by improving input data, different balance of false positives and negatives, or using different learning algorithms) The AI system is tested using new data set(s) to confirm the same outcome is reached. There is evidence to confirm that regular compliance checks are undertaken to provide assurances of statistical accuracy	False acceptance rates and false rejection rates reporting (graphs / charts)
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.	**Buyer** - To ensure there are procedures to allow data subjects to challenge AI outputs and automated decisions and that complaints are documented and managed appropriately with feedback and communications to the system developer where necessary.	Without mechanisms to allow complaints to be recorded, shared and investigated collaboratively between AI stakeholders, there is a risk that AI systems continue to generate inaccurate and uncorrected	There is a log of all complaints received that tracks the issue, the response and the response date There is evidence that analysis has been undertaken on complaints to determine trends, issues and risks There is an action plan or risk register in place to track issues to resolution	Client remediation action plan Compliants log Risk register

	<u>Builder</u> - To ensure there are routes to allow AI system users to alert developers over challenges to AI output and automated decisions by data subjects and that there is a documented and strategic approach to reviewing complaints, making necessary adjustments, retesting and redeploying.	output. **Non conformance with Article 22 UKGDPR.**	Lessons learned feed back into AI system retraining or development	
			There is senior management oversight of complaint trends	

Control	Control Objective	Risk	Indicators	Suggested Evidences or Documentation
1. There is evidence that the potential for discriminatory outputs has been considered and mitigated prior to the 'go-live' decision.	**<u>Buyer</u>** - To ensure that when an AI system is purchased, the buyer undertakes due dilligence to ensure that they select a system which does not have discriminatory outputs or decisions before its use. **<u>Builder</u>** - To ensure that when building an AI system, the builder has a documented and effective approach to identify discriminatory outputs or decisions prior to go-live and has acted on this to mitigate the risk.	Without effective consideration and action taking place there is a risk discrimination may not be identified during the development phase, and will make its way into the final product unmitigated. **Non compliance with Article 5 (1) (a).**	There is a policy / documented process in place that includes details of how the system will be tested prior to implementation	System design documents DPIA for discrimination or bias Due diligence checklists Due diligence reports
			Risks are drawn from policy, user research and design, and computer science expertise.	
			Builder: For biometrics systems or systems potentially processing SCD, discrimination and bias are considered right from the start of the design phase	
			Due diligence by the buyer / assessments by the builder includes all the relevant checks to the design of the AI systems to ensure that there isn't the potential for discriminatory outputs or decisions to be made	
			Due diligence by the buyer / assessments by the builder is conducted by appropriately skilled and experienced technical 'experts'.	
			The results of the due diligence by the buyer / assessments by the builder are documented, including any 'trade offs' and their technical implications	
			Due diligence by the buyer / assessments by the builder are signed off by senior management	
			Checks ensure that there is no imbalance in the training data used to train the system (ie.e over representation of one characteristic / group)	
			The training data is representative of the population or different sets of data subjects that the AI system will be applied to. For example, by comparing against the most recent census.	
			Checks are undertaken to ensure training data does not include any past discrimination	
			The AI system is tested using new data set(s) to confirm the same outcome is reached.	
			There is evidence to confirm that the AI system design has been adapted / changed or retrained following the review where necessary prior to 'go live'.	
2. 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.	**<u>Buyer</u> -** To ensure that the buyer has considered whether the outputs of the system are fair, based on the inclusion of protected characteristics in the decision making process. **<u>Builder</u> -** To ensure that the builder has considered whether they can make the outputs of their system fairer by including the consideration of protected characteristics or special category data by the system as part of any decision making process.	If the system does not make use of personal data to ensure fairness/accuracy (as defined by the goals of the system) there may be a risk, depending on the nature of the processing undertaken by the AI, that data subjects could face inaccurate or unfair results. **Non compliance with Article 5 (1) (a).**	Protected characteristics are included in the AI model where appropriate / necessary to ensure the system does not discriminate against these characteristics.	
			These characteristics are tested thoroughly to ensure they produce the right outputs consistently	
			The protected characteristics included are documented, and the decision making process and risks this has mitigated are recorded in the DPIA.	
			There has been consideration of any 'anti-classification', identifying and excluding proxies for certain protected characteristics	
			Data about under / overrepresented groups undergoes thorough analysis to ensure no discriminatory decisions or outputs are made. The data is removed or deleted if justification can not be made to retain it.	
			SDK's have been designed with 'accessibility' in mind e.g. to meet the needs of individual's with disabilities	

			If a decision was made not to include protected characteristics to reduce bias / discrimination, there has been an assessment of the disproportionate effort to ask for additional data from users in order to proactively include protected characteristics	
3. 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.	To ensure there is a process in place documenting how the expert / peer review of AI system design for discriminatory outputs or decisions made by AI systems should be undertaken and that this review is completed in a timely manner. *Note: This control will depend on the maturity of systems and practical implementation of it - testing can happen in real time as code develops - there should be accountability within the development team to ensure system code / model is reviewed as it is developed by various people in the team.*	Without an independent review of the system design there is a risk of bias or discriminatory outputs being inbuilt into the system. **Non compliance with Article 5 (1) (a).**	There is a documented process in place covering how independent testing of the system will be undertaken to identify any discriminatory outputs or bias The process includes a schedule for testing The process outlines which roles should retain responsibility for the testing and these roles can demonstrate independence. Staff with responsibility for independent testing receive periodic training on new technologies, advancements in technological capabilities and system design to ensure they are able to undertake appropriate and meaningful testing for discrimination and bias in the system. The evaluation of the system includes consultation with both privacy and technical personnel	Quality control process / policy Test plans for discrimination or bias testing Test reports / results
4. There is ongoing monitoring of the AI system to ensure there are no discriminatory outputs or decisions being made.	**Buyer** - To ensure that the buyer has put in place measures to prevent discriminiation taking place after the AI system goes live. **Builder** - To ensure that systems are designed to allow for and facilitate ongoing monitoring for discrimination after the system goes live. To check that the builder does not rely on one testing mechanism only, but uses different / varying methods of testing as appropriate.	Without regular monitoring of the system, there is a risk the system outputs will be 'unfair'. **Non compliance with Article 5 (1) (a).**	There is a documented process for the ongoing monitoring of the system for discrimination and bias. There is a test plan in place to demonstrate the ongoing monitoring is taking place in practice Results of ongoing monitoring are documented Ongoing monitoring includes comparing outcomes for various groups Ongoing monitoring tests include analysis of data about under / overrepresented groups to ensure no discriminatory decisions or outputs are made. The data is removed or deleted if justification can not be made to retain it. Data which reflects past discrimination is modified or deleted from the system if no longer relevant to the current decision. Tests include running a traditional decision-making system and a AI system concurrently and investigations of any significant difference in the type of decisions. There has been consultation with any external experts / reviewed academic literature to help / inform testing strategies for bias - there is not a reliance on one testing mechanism only, instead there are different / varying methods of testing as appropriate.	
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.	**Buyer** - To ensure that there are processes in place for a buyer to take appropriate action should there be any discriminatory outputs that they identify or are identified by users (e.g. through complaints received). Also to provide feedback to the builder for addressing	Without processes to take action and escalate discriminatory outputs identified as part of ongoing montoring, there is a risk that these issues will go unnoticed or unactioned. Without a clear threshold for outputs which would trigger action, there is a	There is a policy / documented process in place that includes details how any new issues as a result of testing will be investigated and mitigated.	

	where it is appropriate to do so. **Builder** - To ensure that the builder has processes in place to outline how they will deal with any identified discriminatory outputs as a result of ongoing monitoring, which could include thresholds in which outputs would require action, what signs staff should look out for that could indicate a discriminatory output and how staff can notify relevent personnel about discriminatory outputs they identify,	risk that builders will spend time trying to address minor issues. **Non compliance with Article 5 (1) (a)**	There are policies in place that set out the tolerance levels of discriminatory outputs (including clear variance limits above which the AI system stops being used), as well as escalation and variance investigation procedures.
			Processes are in place to ensure Client & BPO (processors) feedback is captured and acted on where bias is identified by Client / BPO's
6. Processes are in place to combat any new privacy issues that may be triggered as a result of testing for bias and discrimination.	To ensure that there are documented and effective approaches in place to combat any new privacy issues that arise after testing for bias and discrimination.	If no mitigation strategies are in place, the organisation risks that new privacy issues may go unrestrained, causing direct harm to data subjects. **Non compliance with Article 5 (1) (a).**	There are documented mitigation strategies in place for issues identified as part of ongoing testing
			There is evidence to confirm that the AI system has been 'retrained' following testing (e.g. by implementing algorithmic fairness measures / fairness constraints)
			The AI system is tested using new data set(s) to confirm the same outcome is reached.
			The DPIA is revisited if new privacy issues are triggered and a new assessment is undertaken.
			The learning process is changed and the system is retrained if any 'unfairness' is identified.

Control	Control Objective	Risk	Indicators	Suggested Evidences or Documentation
1. Human reviewers have appropriate knowledge and experience, authority and independence within the organisation to challenge decisions.	**<u>Buyer</u>** - To ensure that the buying organisation has appointed human reviewers with sufficient operational independence. **<u>Builder</u>** - To ensure that the organisation developing the AI software has built in functionality to allow for clients to appoint human reviewers with operational independence.	Without the existence of human reviewers, with the appropriate levels of operational independence and training there is a risk that a human review will not be undertaken, or that the reviews completed are ineffective.	AI system developers understand the skills, experience and ability of human overseers when designing the AI system.	Training material for (sub) processors / BPO analysts Onsite and remote audit plans and reports of processors / BPO (human reviewers) - cold case and real time. QC Process
			Human reviewers have the appropriate technical understanding to understand the decision making behind algorithm (s) used.	
			Human reviewers work with a manageable caseload and there is sufficient resource in place for them to give appropriate time to their tasks.	
			There is a documented analysis of the time expected for a human to conduct a meaningful review.	
			Human reviewers are able to challenge and override automated decision making.	
			Human reviewers receive regular specialised training.	
			Human reviewers are able to work with independence and are able to influence senior-level decision making. These reporting lines are reflected both in job description and in the organisation's framework.	
2. There is a process in place to ensure periodic assessments of the outcomes of human reviews of the AI system(s) and these assessments take place in practice.	**<u>Buyer</u>** - To ensure periodic assessments are completed on the work of / outputs from human reviewers. **<u>Builder</u>** - To ensure that developers build functionality into the AI system to allow for periodic assessments of the outputs of human reviewers.	Without periodic reviews of the work done by human reviewers there is a risk that there is non meaningful human review.	There are separate builder and buyer human review processes	Mystery shopping reports Human review testing plan Human review testing reports
			There is evidence of 'mystery shopping' exercises, where deliberately misleading data is provided that the human should disagree with the AI, to	
			Pre and post implementation testing includes an assessment of human oversight to ensure it is meaningful.	
			A sample of decisions are tested to ensure the human is making the right decision.	
			Decisions made by AI are monitored and compared to human decisions, any action taken as a result of performance which goes outside of defined tolerances is documented.	
			Tests are documented, including how the sample was selected / criteria used.	
			There is evidence to support a re-review or overturning of decisions (e.g. if there is one rogue reviewer)	
3. 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 AI system.	Where the AI system is continuously learning from decisions made, to ensure that the the use of human reviewers does not artificially introduce errors or other deficiencies to future decisions made by the AI system.	The use of human reviewers may result in a corruption of the AI system, and result in inaccuracies or errors being introduced which would otherwise not have existed. In order to avoid this, the controller must ensure there are proper controls to monitor the effects their human review has on the outputs of the AI system.	There has been a mapping of the processing activity of the AI system to identify points where a human review would be appropriate and beneficial	Human review policy and procedures Review risk registers
			Prior to initiating a human review at a certain stage, there has been testing to check the review will not create / cause any new risks to the system	
			Risks identified as a result of a review are logged and actioned / mitigated	
			Where the review has been outsourced, checks are in place to ensure the reviews are done at appropriate stages	
4. 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).	To ensure that where an error is detected by human reviewers, the organisation has documented plans in place for how to rectify the processing and ensure accuracy going forwards.	If there is no agreed process in place to rectify individual or systematic errors in decision making, the organisation may be put in the position of having to cease processing or risk breaching the requirements of the UKGDPR.	There has been a consideration of a 'fall back ' option should reviewers find an issue that questions the competency of the system	Fallback procedures
			The fall back option has been approved by all parties in advance	
			The option is tested periodically to ensure it remains fit for purpose	
			There is an agreed 'stand in' time for the alternative option to allow time for developers to rectify the issues with the AI system	
			Incase of service failure, is there flexibility to move to a hybrid or manual model - automated processing first, then manual check.	
			If levels / tolerance set for auto processing decisions fall below acceptable levels, this triggers a manual review.	

Control measures	Evidences			Assurance	Report Text					QA
	Documentation	Interview	Testing	Rating	Findings	Non Conformities	Recommendations	Priority	Best Practice	QA Comments
Trade Offs										
1. 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.				Green	hbgivboiu	nfvo inbwfp iowbnf	dvbn owb ow	Urgent		
2. Decisions made during the trade off analysis have been documented and signed off at an appropriately senior or expert level.										
3. As part of model and system 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).										
4. 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.				Green						
Statistical Accuracy										
1. The organisation has methods in place to ensure that the data sets relied on for determining statistical accuracy are accurately and fairly labelled.				Yellow						
2. There is pre-implementation statistical accuracy testing of new AI 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.										
3. 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.										
4. Post-implementation testing is carried out and the results of the testing and action(s) taken as a result are documented.										
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.				Green						
Discrimination & Bias										
1. There is evidence that the potential for discriminatory outputs has been considered and mitigated prior to the 'go-live' decision.				Yellow						
2. 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.										
3. 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.										
4. There is ongoing monitoring of the AI system to ensure there are no discriminatory outputs or decisions being made.										
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.										
6. Processes are in place to combat any new privacy issues that may be triggered as a result of testing for bias and discrimination.				Green						
Human Review										
1. Human reviewers have appropriate knowledge and experience, authority and independence within the organisation to challenge decisions.				Red						
2. There is a process in place to ensure periodic assessments of the outcomes of human reviews of the AI system(s) and these assessments take place in practice.				Red						
3. 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 AI system.				Red				Low		
4. 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).				Red				Urgent		

Governance

Control measures	Non Conformities	Recommendations	Priority
There is an embedded privacy management framework endorsed by senior management that supports the use of AI systems.	nfvo inbwfp iowbnf	dvbn owb ow	Urgent
Technical and operational roles and responsibilities have been assigned to support the day to day management of all aspects of AI systems	dnbc owowbonwdbwd wd kjwbd nivhwuoihvwuv iuhvwiubvhweouhro iuhv woeruhv wo o	cdbiwudhbgcou hwouwdhuo uoehvcouewhv oow weouihv ohwo	High
Privacy considerations and measures for AI development and implementation are set out in a framework of policies and procedures.	dwjv howiuhjoeihcnv ldlo vowh bouwhouvhfehvbnbeuhvo viov uv hwowh ohig wuhv hwdiv hwiuhve gouwg owuh iwgiuwe hvogiuhwdouh	fjb oue hgv,wrkli iuhr otyhg oe;uthoeh ; iuhrg ;uerh ierggreh glier lierhg luerh gherl	Medium
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	0	0	0
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.	0	0	0
Change management processes are documented in policy to ensure that new versions or change releases to AI systems are managed effectively by all parties	0	0	0
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.	0	0	0
Data flows across the entire supply chain have been comprehensively mapped.	0	0	0

Transparency

Control measures	Non Conformities	Recommendations	Priority
Appropriate and timely privacy information is provided to individuals.	0	0	0

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)	0	0	0
Existing AI privacy information is regularly reviewed and, where necessary, updated appropriately.	0	0	0
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 AI systems on a regular basis.	0	0	0

Lawful Basis

Control measures	Non Conformities	Recommendations	Priority
The most appropriate Article 6 lawful basis (or bases) and Article 9 or 10 condition have been identified for each processing activity within the AI system.	0	0	0
A legitimate interests assessment has been undertaken where there is a reliance on legitimate interests as a lawful basis.	0	0	0
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.	0	0	0

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.	0	0	0
There are processes in place to identify the potential use or processing of children's data in AI systems and children's data is not used unless there is a lawful basis to do so.	0	0	0
Processes are in place to ensure that marketing to data subjects as a result of profiling within AI systems is lawful.	0	0	0
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.	0	0	0
There is evidence of a periodic review of documented lawful bases to ensure their continued validity.	0	0	Urgent

Contracts & 3rd Parties

Control measures	Non Conformities	Recommendations	Priority
There has been a full consideration of the controller/processor/ joint controller relationship throughout the whole supply chain in the use of AI systems	nfvo inbwfp iowbnf	dvbn owb ow	Urgent
The decision reached on the controller / processor relationship across all proposed processing activities is documented.	0	0	0

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.	0	0	
Where the use of an AI system results in the creation and therefore processing of new attributable personal or special category data, due diligence checks are undertaken to ensure that individuals have either already received appropriate privacy information or else are provided with it in a timely manner.	0	0	
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 AI systems.	0	0	
There is an appropriate level of due diligence undertaken prior to any arrangement being agreed to ensure that appropriate measures will be in place to protect and enable individual rights	0	0	
When procuring AI systems or services, there is evidence that the buyer has considered what their acceptable level of system output accuracy is and has completed due diligence to ensure the product meets these accuracy requirements.	0	0	
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).	0	0	

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.	0	0	
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.	0	0	
Contracts are managed and reviewed	0	0	
Written contracts include all the details, terms and clauses required under the UK UKGDPR	0	0	
There is in-life contract monitoring or one-off arrangement reviews to ensure partners abide by agreements	0	0	
PROCESSOR ONLY: 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.	0	0	
PROCESSOR ONLY: 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.	0	0	

Minimisation

Control measures	Non Conformities	Recommendations	Priority

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.	0	0	0
There is ongoing monitoring and testing of data use to ensure only the minimum data required is being processed by the AI system.	0	0	0
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.	0	0	0
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).	0	0	0

Individual Rights

Control measures	Non Conformities	Recommendations	Priority
There is evidence of a policy / process for dealing with individual rights (IR) requests in the data processing pipeline	0	0	0
There is documented guidance available for data subjects on how to make a request.	0	0	0
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.	0	0	0
The organisation systematically monitors the time taken to respond to requests in order to identify systems which are potentially more complex.	0	0	0

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	0	0	0
There is a process and the technical capability in place to action any requests by individual's to cease processing their data within the AI system(s).	0	0	0
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).	0	0	Urgent

Staff Training

Control measures	Non Conformities	Recommendations	Priority
BUILDER: All key roles in the design, development and testing of AI systems have received appropriate training in data protection and information security.	nfvo inbwfp iowbnf	dvbn owb ow	Urgent
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.	0	0	0
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.	0	0	0
Staff within both technical and privacy roles continually develop and maintain up to date skills and knowledge to enable them to effectively fulfil their responsibilities in their role(s).	0	0	0
Training has been provided to individuals involved in the assessment of lawful bases.	0	0	0

All functions and individuals responsible for the development, testing, deployment and monitoring of AI systems are adequately qualified to understand the associated statistical accuracy requirements and measures	0	0	0
There is evidence that AI developers and human reviewers are adequately qualified to identify and address bias and discrimination in AI systems.	0	0	0
AI systems developers receive training and have access to guidance on the requirement to consider individual rights (IR) at the offset.	0	0	0
Customer facing staff receive training on Chapter 3 of the UK GDPR on individual rights, and there are appropriate SOPs / procedures in place. The training or procedures include how to escalate more complex requests.	0	0	0
BUYER: 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 prior to and during the use of the AI system their organisation has purchased.	0	0	0

DP Risk Management

Control measures	Non Conformities	Recommendations	Priority
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.	0	0	0
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.	0	0	0

There is a DPIA policy / process in place, with supporting templates and guidance to facilitate the completion of an effective DPIA that meets the requirements under the UKGDPR (Article 35)	0	0	0
There is evidence that internal stakeholders, technical specialists within AI product teams and data subjects (or their nominated representative(s)) have been consulted as part of the DPIA assessment as appropriate.	0	0	0
Appropriate senior management have oversight of completed DPIA reports and sign off on the outcome of the assessment.	0	0	0
The outputs of a DPIA are acted upon to effectively mitigate or manage any risks identified.	0	0	0
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.	0	0	0
There is an effective risk management strategy in place to facilitate the formal documentation of risks associated with the use of AI systems and ensure they are tracked and managed at a corporate level through an appropriate risk register	0	0	0
There is evidence that risks are being mitigated through ongoing AI system development / enhancements	0	0	0

Security & Integrity

Control measures	Non Conformities	Recommendations	Priority
There has been a thorough assessment of security risks to or in the AI system prior to its implementation to reduce the likelihood of an attack or breach	0	0	0
Security measures are in place to prevent privacy attacks on Machine Learning (ML) models through model inversion, membership inference or adversarial examples.	0	0	0

There is ongoing monitoring of the AI system for software vulnerabilities. Security fixes are applied where appropriate.	0	0	0
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).	0	0	0
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.	0	0	0
The organisation has effective asset management processes in place to ensure a coordinated approach to the security of data within it's systems.	0	0	0
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.	0	0	0
There is evidence of a policy / processes for data breach reporting and escalation.	0	0	0
The organisation monitors systems/network activity to detect suspicious requests and **take action as a result**.	0	0	0
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.	0	0	0
The organisation has in place effective mechanisms in order to prevent unauthorised access (read/write), or inappropriate changes being made to data sets.	0	0	0
The organisation has in place effective mechanisms in order to monitor and track all changes being made to personal data.	0	0	0

There are business continuity and disaster recovery plans in place.	0	0	Urgent

Trade Offs

Control measures	Non Conformities	Recommendations	Priority
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.	nfvo inbwfp iowbnf	dvbn owb ow	Urgent
Decisions made during the trade off analysis have been documented and signed off at an appropriately senior or expert level.	0	0	0
As part of model and system 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).	0	0	0
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.	0	0	0

Statistical Accuracy

Control measures	Non Conformities	Recommendations	Priority
The organisation has methods in place to ensure that the data sets relied on for determining statistical accuracy are accurately and fairly labelled.	0	0	0
There is pre-implementation statistical accuracy testing of new AI 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.	0	0	0

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.	0	0	0
Post-implementation testing is carried out and the results of the testing and action(s) taken as a result are documented.	0	0	0
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.	0	0	0

Discrimination & Bias

Control measures	Non Conformities	Recommendations	Priority
There is evidence that the potential for discriminatory outputs has been considered and mitigated prior to the 'go-live' decision.	0	0	0
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.	0	0	0
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.	0	0	0
There is ongoing monitoring of the AI system to ensure there are no discriminatory outputs or decisions being made.	0	0	0
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.	0	0	0

Processes are in place to combat any new privacy issues that may be triggered as a result of testing for bias and discrimination.	0	0	0

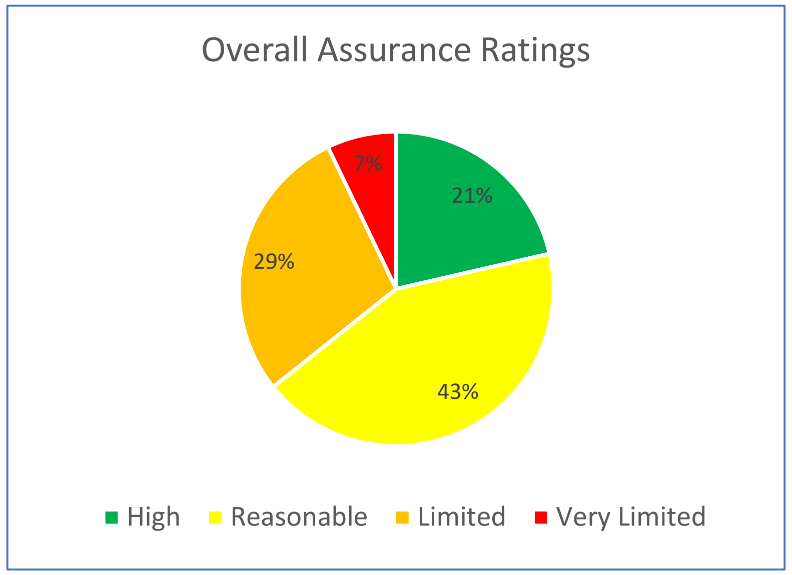
Human Review

Control measures	Non Conformities	Recommendations	Priority
Human reviewers have appropriate knowledge and experience, authority and independence within the organisation to challenge decisions.	0	0	0
There is a process in place to ensure periodic assessments of the outcomes of human reviews of the AI system(s) and these assessments take place in practice.	0	0	0
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 AI system.	0	0	Low
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).	0	0	Urgent

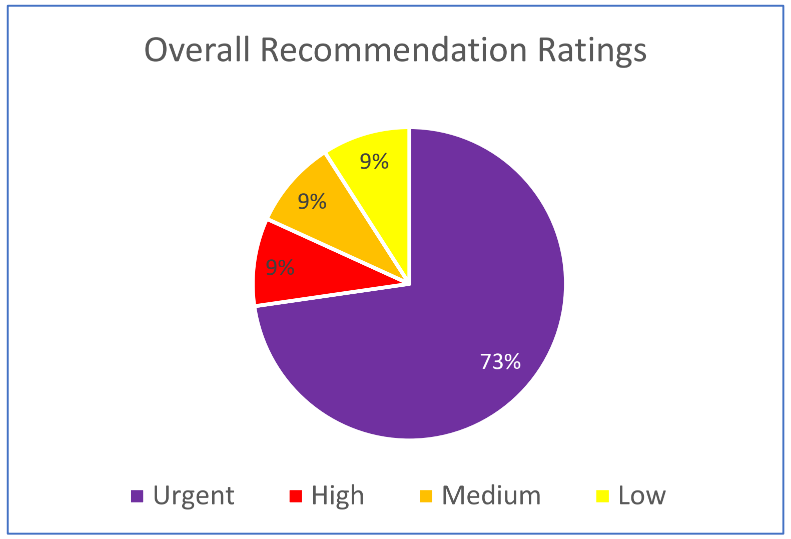
Table showing assurance rating by domain

Domain	Assurance Rating	Overall Opinion
Governance	Reasonable	
Transparency	Reasonable	
Lawful Basis	Limited	
Contracts & 3rd Parties	High	
Data minimisation	Reasonable	
Individual Rights	Limited	
Staff Training	High	
DP Risk Management	Reasonable	
Security & Integrity	Limited	
Trade Offs	High	
Statistical Accuracy	Reasonable	
Discrimination & Bias	Reasonable	
Human Review	Very Limited	

Pie chart showing split of ratings



Pie chart showing overall recommendation ratings



Green	1	0	0	0	1		2.2	Urgent	2	Urgent	2	Green
Yellow	0	2	0	0	2		Reasonable	High	1	High	1	Yellow
Amber	0	0	3	0	3			Medium	1	Medium	1	Amber
Red	0	0	0	4	4			0	0	Low	1	Red
0	0	0	0	0	0			0				
0	0	0	0	0	0			0				
0	0	0	0	0	0			0				
Green	1	0	0	0	1			0				
0	0	0	0	0	0			0				
Yellow	0	2	0	0	2		1.5	0			1	Green
0	0	0	0	0	0		Reasonable	0			1	Yellow
0	0	0	0	0	0			0			0	Amber
Green	1	0	0	0	1			0			0	Red
0	0	0	0	0	0			0				
Yellow	0	2	0	0	2		3	0			0	Green
0	0	0	0	0	0		Limited	0			1	Yellow
0	0	0	0	0	0			0			0	Amber
0	0	0	0	0	0			0			0	Red
0	0	0	0	0	0			0				
0	0	0	0	0	0			0				
0	0	0	0	0	0			0				
Red	0	0	0	4	4			Urgent				
Green	1	0	0	0	1		1	Urgent	2	Urgent	2	Green
0	0	0	0	0	0		High	0	0	High	0	Yellow
0	0	0	0	0	0			0	0	Medium	0	Amber
0	0	0	0	0	0			0	0	Low	0	Red
0	0	0	0	0	0			0				
0	0	0	0	0	0			0				
0	0	0	0	0	0			0				
0	0	0	0	0	0			0				
0	0	0	0	0	0			0				
0	0	0	0	0	0			0				
0	0	0	0	0	0			0				
0	0	0	0	0	0			0				
0	0	0	0	0	0			0				
0	0	0	0	0	0			0				
Green	1	0	0	0	1			0				
0	0	0	0	0	0			0				
Yellow	0	2	0	0	2		1.5	0			1	Green
0	0	0	0	0	0		Reasonable	0			1	Yellow
0	0	0	0	0	0			0			0	Amber
Green	1	0	0	0	1			0			0	Red
0	0	0	0	0	0			0				
Yellow	0	2	0	0	2		3	0			1	Green
0	0	0	0	0	0		Limited	0			1	Yellow
0	0	0	0	0	0			0			0	Amber
0	0	0	0	0	0			0			1	Red
0	0	0	0	0	0			0				
0	0	0	0	0	0			0				
Red	0	0	0	4	4			Urgent				
Green	1	0	0	0	1		1	Urgent	2	Urgent	2	Green
0	0	0	0	0	0		High	0	0	High	0	Yellow
0	0	0	0	0	0			0	0	Medium	0	Amber
0	0	0	0	0	0			0	0	Low	0	Red
0	0	0	0	0	0			0				
0	0	0	0	0	0			0				
0	0	0	0	0	0			0				
0	0	0	0	0	0			0				
0	0	0	0	0	0			0				
Green	1	0	0	0	1			0				
0	0	0	0	0	0			0				
Yellow	0	2	0	0	2		1.5	0			1	Green
0	0	0	0	0	0		Reasonable	0			1	Yellow
0	0	0	0	0	0			0			0	Amber
0	0	0	0	0	0			0			0	Red
0	0	0	0	0	0			0				
0	0	0	0	0	0			0				
0	0	0	0	0	0			0				
0	0	0	0	0	0			0				
Green	1	0	0	0	1			0				
0	0	0	0	0	0			0				
Yellow	0	2	0	0	2		3	0			0	Green
0	0	0	0	0	0		Limited	0			1	Yellow
0	0	0	0	0	0			0			0	Amber
0	0	0	0	0	0			0			1	Red
0	0	0	0	0	0			0				
0	0	0	0	0	0			0				
0	0	0	0	0	0			0				
0	0	0	0	0	0			0				
0	0	0	0	0	0			0				
0	0	0	0	0	0			0				
0	0	0	0	0	0			0				
0	0	0	0	0	0			0				
Red	0	0	0	4	4			Urgent				
Green	1	0	0	0	1		1	Urgent	2	Urgent	2	Green
0	0	0	0	0	0		High	0	0	High	0	Yellow
0	0	0	0	0	0			0	0	Medium	0	Amber
Green	1	0	0	0	1			0	1	Low	0	Red
0	0	0	0	0	0			0				
Yellow	0	2	0	0	2		1.5	0			1	Green
0	0	0	0	0	0		Reasonable	0			1	Yellow
0	0	0	0	0	0			0			0	Amber
0	0	0	0	0	0			0			0	Red
Green	1	0	0	0	1			0				
0	0	0	0	0	0			0				
Yellow	0	2	0	0	2		1.5	0			1	Green
0	0	0	0	0	0		Reasonable	0			1	Yellow
0	0	0	0	0	0			0			0	Amber
0	0	0	0	0	0			0			0	Red
0	0	0	0	0	0			0				
Green	1	0	0	0	1			0				
0	0	0	0	0	0			0				
Red	0	0	0	4	4		4	0			0	Green
Red	0	0	0	4	4		Very Limited	0			0	Yellow
Red	0	0	0	4	4			Low			0	Amber
Red	0	0	0	4	4			Urgent			4	Red
						High	3	8	Urgent			
						Reasonable	6	1	High			
						Limited	4	1	Medium			
						Very Limited	1	1	Low			

Green	Urgent	There is a high level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified only limited scope for improvement in existing arrangements and as such it is not anticipated that significant further action is required to reduce the risk of non-compliance with data protection legislatic
Yellow	High	There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.
Amber	Medium	There is a limited level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified considerable scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.
Red	Low	There is a very limited level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified a substantial risk that the objective of data protection compliance will not be achieved. Immediate action is required to improve the control environment.
N/A	N/A	N/A

Table showing assurance rating by domain

Domain	Assurance Rating
Governance	Reasonable
Transparency	Reasonable
Lawful Basis	Limited
Contracts & 3rd Parties	High
Data minimisation	Reasonable
Individual Rights	Limited
Staff Training	High
DP Risk Management	Reasonable
Security & Integrity	Limited
Trade Offs	High
Statistical Accuracy	Reasonable
Discrimination & Bias	Reasonable
Human Review	Very Limited

Pie chart showing ratings split

High	3
Reasonable	6
Limited	4
Very Limited	1

Pie chart showing overall recommendation ratings

Urgent	8
High	1
Medium	1
Low	1

Document Control Panel:

Document name/title	Artificial Intelligence (AI) Working Paper - Master version
Version number	1.0
Status (draft, published or superseded)	Published
Department/Team	Assurance (Audit)
Relevant or related policies	N/A
Distribution (internal or external)	Internal
Author/Owner (if different name both)	Leanne Doherty (Author) Assurance (Owner)
Approved by	Leanne Doherty
Date of sign off	14/3/22
Review by	14/3/24
Security classification	Official

Version History Panel:

Version	Changes made	Date	Made By
1.0	**Document Control Panel and Version History Panel added. Uploaded to SharePoint**	**14/3/22**	**L.Doherty**