



مصرف الإمارات العربية المتحدة المركزي
CENTRAL BANK OF THE U.A.E.

**Guidance Note on the Consumer Protection and
Responsible Adoption and Use of Artificial Intelligence and
Machine Learning by Licensed Financial Institutions in the
U.A.E.**

Table of Contents

1	Definitions	2
2	Governance and Accountability.....	3
3	Fairness/Non-Discrimination and Ethics	3
4	Transparency and Explain ability	4
5	Data Quality, Privacy and Security	4
6	Continuous Monitoring and Review	5
7	Human Oversight and Consumer Protection	5
8	Integration with Existing Frameworks.....	6
9	Outsourcing and Third-Party Risk.....	6
10	Ethical Collaboration and Innovation	7

Guidance Note on the Consumer Protection and Responsible Adoption and Use of Artificial Intelligence and Machine Learning by Licensed Financial Institutions in the U.A.E.

This Guidance Note outlines principals and guidelines for the use of Artificial Intelligence (AI) systems and Machine Learning (ML) technologies by licensed financial institutions, including insurance providers (LFIs), in the United Arab Emirates (the UAE). It is focused on areas that may have bearing on consumers, with the aim of promoting consumer protection and good market conduct by all LFIs in their use of AI/ML.

Given the continued and rapid development of AI and ML, both generally and as adopted by LFIs, these broad principles and guidelines should not be taken to be static or fixed, but rather as flexible principles to be used to guide and inform responsible AI/ML use over time as the sector, deployment and use of AI/ML develops. Though this Guidance Note is focused on consumer protection in particular, the CBUAE urges LFIs to consider the consequences of AI/ML from a broader perspective, including financial and nonfinancial risk management as well.

The objective of this Consumer Protection Guidance Note is to encourage a culture of responsible and ethical use, transparency and innovation with a focus on the end user in the development, deployment and use of AI and ML technologies, models and systems by LFIs.

This Guidance Note is non-binding and sets out principles and guidance to assist LFIs in formulating their own policies and procedures. It is expected LFIs will refer to this Guidance as they develop their own internal policies and guidance on the ethical and responsible use of AI and ML with respect to consumers.

This guidance takes into account the UAE Charter for the Development & Use of AI, published in July 2024, the UAE National Strategy for AI, and the Central Bank Guidelines for Financial Institutions adopting Enabling Technologies.

1 Definitions

For the purpose of this Guidance Note, the following terms shall have the meanings set forth below:

- **Artificial Intelligence (AI)** means computer or machine-based systems or models that perform tasks or generate outputs normally requiring human intelligence, including learning, reasoning, understanding, and interacting and GenAI (as defined below) which may have varying levels of autonomy and/or the ability to learn from data and adapt.
- **GenAI** means artificial intelligence models that can understand and generate human like text, audio and images by leveraging vast amounts of training data and deep learning techniques, including popular Large Language Models.
- **Machine Learning (ML)** means a subset of AI that enables systems to learn, both as supervised and unsupervised learning, from data and improve performance without being explicitly programmed or instructed to do so.
- **High-impact decision** means any determination by an LFI using AI that materially affects a customer's access to financial products or services, for example in respect of a potential loan application or insurance claim.

2 Governance and Accountability

- a. LFIs should adopt a documented governance framework for AI and ML that is commensurate with the size, nature and complexity of their operations. A culture of responsible use of AI with an understanding of the risks of it should be promoted in LFIs. This Guidance should be read in conjunction with all relevant CBUAE regulations and standards.
- b. Senior management and the Board of Directors of LFIs should be responsible and accountable for AI and ML systems and outcomes, model selection/development, deployment, accountability, appropriate human resourcing and oversight and monitoring and management on an on-going basis.
- c. Regular reporting should be required by and provided to Senior Management and Boards of LFIs, covering performance and risk.
- d. Governance structures should facilitate informed decision-making, enable the identification and mitigation of risks and ensure that AI and ML systems and applications are aligned with the institution's risk appetite and legal obligations. AI-related risks should be incorporated into the institution's governance framework in a cohesive and consolidated manner, including with specific adaptable roles and responsibilities for the Audit and Risk Committee, Risk Management, Internal Audit, and IT.
- e. Boards and senior management should ensure that risk committees and control functions (e.g., compliance, internal audit and risk management) understand AI-driven processes and can challenge outcomes where appropriate, with the adoption, deployment and use of AI being an integral part of the Risk Management framework.
- f. An inventory of all AI models, systems or technologies developed or deployed should be maintained and embed compliance measurers and training in all functions responsible for the use, management, and monitoring of the same, which should follow the CBUAE Model Management Standards and Model Management Guidance (2022). Such inventory should contain all material metadata, to include as a minimum model name, purpose, risk rating. A tool LFIs may wish to consider for use is the Shapley Additive Explanations (SHAP), to explain the output of models, or any other well-documented approaches to enhance algorithmic transparency.

3 Fairness/Non-Discrimination and Ethics

- a. LFIs are expected to ensure that AI and ML systems do not result in discriminatory or manipulative outcomes against individuals or groups. No AI system or application should be deployed or used if it is discriminatory or manipulative or develops as such post-deployment.
- b. Data used to train AI and ML models should be sufficiently accurate, relevant and representative of the customer populations to which the models will be applied.
- c. AI deployed should be subject to periodic testing, i.e. once a year or each time a model is upgraded, materially changed or a new one is introduced, to identify and remediate undue/unintended embedded biases or discriminatory outcomes. The deployment of AI should reflect the institution's ethical standards and code of conduct. Decisions made or supported by AI should be consistent with the duty to act honestly, fairly and in the best interests of consumers.

4 Transparency and Explain ability

- a. LFIs should be transparent with customers and relevant stakeholders about the use of AI, particularly in respect of high-impact decisions, and if they are communicating or interacting with an AI application. LFIs should be clear as to how AI systems operate and make decisions and be able to disclose the same.
- b. Institutions should maintain documentation relating to the design, training data, model assumptions and functioning of AI to facilitate internal review and internal and external audit.
- c. Understandable plain language and accurate disclosures should be made in both Arabic and English, with telephone support available in all major languages of the UAE. LFIs should consider the use of appropriate measures to check understandability, such as the SMOG index or Flesch-Kincaid index, or any other well-documented approaches to provide insights into and analysis of disclosures to consumers.
- d. LFIs should provide customers with meaningful information regarding the logic of AI decisions and make available mechanisms for customers to seek clarification or redress.
- e. LFIs should consider the provision of opt-out rights with respect to AI for customers, particularly for High-impact decisions, taking into account the potential risks or impact to the customer, fairness and feasibility.

5 Data Quality, Privacy and Security

- a. LFIs should ensure that data used in AI and ML models is of sufficient quality and relevance and is updated as necessary, in compliance with all relevant standards, laws and regulations (including the UAE Personal Data Protection Law (Federal Decree Law No. 45 of 2021 as amended, supplemented and all executive regulations published in connection with this).
- b. Personal data should be collected, stored and used in compliance with applicable laws and regulations, and only for purposes that are legitimate and proportionate and in respect of outsourcing LFIs should see section 10 below.
- c. Institutions should incorporate privacy-by-design and security-by-design principles into AI systems and maintain safeguards to protect data from unauthorised access or misuse.
- d. Robustness and safety should be integral to AI development. AI should be subject to stress testing and validation to ensure they operate reliably under a range of scenarios and do not produce unsafe or unintended outputs. Institutions should incorporate operational resilience measures—such as redundancy, contingency planning and incident response—to minimise disruption or harm to consumers from system failures or cyber-attacks.
- e. LFIs should assess and try to utilise, where feasible, AI to identify potential fraud or criminal activity, anti-money laundering disparities or issues and potential suspicious activity through trends and patterns and in the event material findings are identified, comply with their legal, regulatory and reporting requirements.

6 Continuous Monitoring and Review

- a. AI should be subject to continuous monitoring to ensure ongoing understanding, reliability, relevance and alignment with consumer protection objectives.
- b. LFIs are expected to consistently monitor and review and, where appropriate, update or cease using AI and ML models, taking into account changes in data, market conditions and customer behaviors. Independent third-party providers of AI, independent experts and third parties (willing to challenge and question the use of AI in an LFI) should be engaged periodically to assess the development of and use of AI including third-party AI providers.
- c. Mechanisms should be in place to detect, report and remediate any performance issues, biases or unintended consequences that may arise over time.
- d. LFIs should remain responsible for outsourced AI functions and should consider: appropriate contractual rights with respect to audit and information rights from providers, be made aware of any material developments with the AI provider, appropriate termination/cease provisions, data protection, cyber security, performance guarantees, its compliance with laws/regulations and standards and any material developments with regard to the AI being outsourced/utilized.
- e. LFIs should at all times retain the clear and immediate ability, with human intervention, to cease use of an AI model system, technology or application deployed or utilized.
- f. LFIs should ensure they have systems in place to keep up to date with legal, third-party provider and market developments with respect to the use of AI.

7 Human Oversight and Consumer Protection

- a. LFIs should ensure that AI and ML systems operate under meaningful human oversight and judgement, particularly for decisions that have significant implications for consumers and in respect of the ongoing selection of, determination as to third party providers of, deployment of and ongoing monitoring and general use of AI. Human oversight may be exercised through different models: (i) **Human-in-the-loop** – where a AI provides recommendations but a human decision maker retains full authority to approve or reject the outcome; (ii) **Human-on-the-loop** – where the AI works autonomously for routine tasks, while a human monitors outcomes and can intervene where necessary; and (iii) **Human-out-of-the-loop** – where the AI operates without direct human involvement, which should only be utilised for low-risk, non-material processes with appropriate controls in place.
- b. The level of human involvement should be commensurate with the identified and potential risks posed to a consumer by any AI.
- c. Consumers should be able to request human review or explanation of AI generated decisions, and alternative arrangements should be available where a customer does not wish to be subject to an AI decision. LFIs should maintain clear and accessible channels for complaints and redress in line with Article 8 of the Consumer Protection Regulation. Consumers should be informed of their right to challenge decisions, correct inaccurate data inputs having impact on AI and the process to challenge data and decisions by AI. A clear complaints-handling procedure/policy should be created, provided and accessible by customers on a regular basis. Complaints should be addressed in person, efficiently, confidentially and in as short at time as is reasonable in the circumstances.

- d. The design and deployment of AI and ML systems should promote fair and equitable treatment. AI should not be used to target consumers with unsuitable products or to engage in pressure-selling or misleading marketing. Institutions should ensure that promotional materials and chatbots comply with disclosure requirements, all in line with the Consumer Protection Regulation's emphasis on good disclosure.

8 Integration with Existing Frameworks

- a. Whilst the focus of this guidance is Consumer Protection, risk management with respect to AI and ML activities should be embedded within the institution's enterprise-wide risk management framework, including conduct risk, credit risk, operational risk and cybersecurity risk. AI risk assessments should not operate in isolation but should inform and be informed by the institution's overall risk appetite and controls.
- b. Senior management should ensure that policies and procedures for AI adoption complement, rather than duplicate, existing regulatory obligations under the Consumer Protection Regulation and other CBUAE directives. For example, consumer risk arising from AI-driven models should be treated as part of the conduct risk framework, with appropriate reporting to the board and regulators.
- c. Where an LFI is developing AI internally, it should consider the use of third-party independent reviews to check suitability, security and reliability.
- d. LFIs should create processes to rate the risk of each AI system/application/technology they deploy or use, to enable appropriate risk assessment, monitoring and management of the AI whilst deployed in use and developing, which may be influenced by data quality and sensitivity, capability of the AI, controls in place, impact of the AI and dependence on the AI and/or third parties in the use of the AI.

9 Outsourcing and Third-Party Risk

- a. Where LFIs rely on third-party vendors or cloud service providers for AI and ML models, products or solutions, due diligence should be conducted on the provider's reputation in the field of AI, governance, security and data-protection practices. Contracts should include provisions that ensure access to relevant information, audit rights and compliance with CBUAE requirements.
- b. The outsourcing of any AI system and/or engagement with third party providers of AI should only be carried out with appropriate diligence, assessment and it should be considered if only to be done by way of Board of Director and/or Senior Management approval, with such processes being appropriately documented for audit purposes.
- c. The procurement, choice and justification for selection of a third-party AI provider and deployment of their AI models/systems/technology at an LFI should be appropriate and documented, which should include annual cybersecurity reviews by independent and suitably qualified third parties and pre-deployment tests and checks to ensure appropriateness and taking into accounts needs, risks and the options available.
- d. Institutions should maintain an inventory of AI models, including those developed or hosted by third parties, and aim to ensure that third-party models adhere to the same standards of fairness, explainability and robustness as in-house models.

- e. LFIs should consider and try to utilise a range of AI providers if feasible, to try to ensure there is no over reliance on one AI system or provider.

10 Ethical Collaboration and Innovation

LFIs are encouraged to collaborate with industry peers (and participate in the UAE AI sandboxes and the Innovation Hub in relation to AI), academia, the CBUAE and other stakeholders to share best practices and to contribute to the development of industry standards for trustworthy AI. LFIs should publish case studies on AI development, responsible use and its interaction with customer care and good market conduct, including any relevant examples which may be provided anonymously.

This Guidance Note is intended to assist LFIs in developing and maintaining policies and procedures for AI that promote responsible innovation, good market conduct and the protection of consumers, notwithstanding the effects that AI/ML could

LFIs are encouraged to stay informed of developments in AI technologies and to engage with the CBUAE where guidance or clarification is required. This Guidance Note shall supplement and not replace any laws, regulations or directives issued by the CBUAE or other competent authorities, and LFIs remain responsible for complying with all applicable laws, regulations and requirements.