Type of Document: *Policy*

Artificial Intelligence (AI) Policy

Owners: CIO, CRO

Date: June, 2022

Version: N. 1

REGISTRY

Type of Document:	Policy	
Owner Unit of the Document	CIO, CRO	
Contacts	CIO: Filipe Teixeira filipe.teixeira@illimity.com	
	CRO: Claudio Nordio claudio.nordio@illimity.com	
Units involved in the internal regulation process of the Document	Compliance & AML; HR & Organization, Strategy, Sustainability & IR	
Recipients of the Document	**Parent Company**	**Subsidiaries Entities**
	illimity Bank S.p.A	All illimity Group's entities
Version approved by	Board of Directors	
Approval Date	15/06/2022	
Validity Date	16/06/2022	

VERSIONS

Regulation Title with # versioning	Main changes	Approving Body and date of approval
Artificial Intelligence Policy V.1	First version of the document	Board of Directors, 15/06/2022

Index

1 INTRODUCTION.....5
2 GLOSSARY.....5
3 PRINCIPLES.....7
4 CLASSIFICATION AND MANAGEMENT MODEL.....8
5 RELATED REGULATION.....11

1 INTRODUCTION

This Policy aims to implement, in coherence with illimity group's business model and core values, the voluntary indications regarding ethical profiles as defined from time to time by the European Union and the Organization for Security and Cooperation in Europe (OECD), specifically regarding the governance of the AI (Artificial Intelligence) models used by the Group, which also undertakes to implement them in compliance with the Information Security rules.

In particular, referring to the European Commission Communication of 25 April 2018 on Artificial Intelligence for Europe, and taking into account the fact that the General Data Protection Regulation (GDPR) became effective on 25 June 2018, as well as the Proposal for a Regulation of the European Parliament and of the Council establishing harmonized rules on artificial intelligence (so-called Law-Act on Artificial Intelligence) of 21 April 2021 (COM (2021) 206 final 2021/0106 (COD)), the illimity Group recognizes the importance of addressing the challenges associated with the use of AI and the ethical implications that derive from it. In this regard, the illimity Group continuously monitors regulatory developments, including the regulatory and guideline levels, for timely implementation and adaptation of its internal regulations, where deemed appropriate.

Furthermore, with regard to the OECD Council Recommendation on Artificial Intelligence, the following chapter defines the principles by which the illimity Group is inspired in its approach to model governance and information security.

2 GLOSSARY

Definitions	
Bank or Parent Company	illimity Bank S.p.A. headquartered in Milan, via Soperga n. 9 – Zip Code 20127
Group	Parent company and its subsidiaries pursuant to and for the purposes of Article 2359 of the Italian Civil Code
Artificial Intelligence	Methodological approach, as defined in paragraph 4 of this document, such that, when implemented informatically for a certain series of targets defined by the developer, it can generate outputs such as contents, forecasts, recommendations, or decisions that influence the environments with which they interact
First and second-tier risks	Risks whose governance (identification, measurement and control, management, mitigation, and reporting) falls within the responsibility of the business / operational functions (first level, where risks are generated) or of the control functions (second level, therefore the risk control function and the compliance and anti-money laundering functions)
AI High Risk Models	AI models which, by virtue of their scope of application, potentially pose significant risks to health and safety or to the fundamental rights of individuals, and for which a solid methodology for the management of these risks must therefore be implemented
Significant Risk Transactions	Transactions that are identified as exceeding a given amount of risk, either individually or when grouped with similar transactions already in place or in the near future (also accumulated over time, classified into types of portfolios of homogeneous financial instruments and which present an overall risk limit, or attributable to the implementation of the

	same strategy). They may relate to the entire operations of the bank and may concern transactions with related parties, as may potentially configure conflict of interest. All operations of an extraordinary nature are included, even if they fall within the specific competence of the Board of Directors.

Acronyms	
AI	Artificial Intelligence
GDPR	UE Regulation n° 2016/679 - General Data Protection Regulation
OECD	Organization for Security and Cooperation in Europe
SRT	Significant Risk Transactions

3 PRINCIPLES

For the purposes of this Policy, the Group undertakes to comply with the application of the best standards in the field of Artificial Intelligence, extending to the whole AI models used by the Group the principles set out to “high risk” models by the Proposal for Regulation of the European Parliament. Therefore, in line with the principles defined by the OECD Observatory and with the ethical guidelines of the European Commission for reliable AI, the Group undertakes to comply with the following guidelines:

a) sustainable development and well-being, achieved by models with higher performance than traditional ones, therefore able to ensure a better selection, assumption, pricing, management, and control of the risks of the funded initiatives, strengthening the mechanisms for the proper functioning of the credit markets and more generally of the economy as a whole;

b) centrality of the human factor, which maintains a primary role in the development and validation of models (with the involvement of the business units in the analysis of the indicators used, their meaning, and the relationship between their valuation and the final credit rating), as well as downstream control through final override processes of a judgmental nature and appropriately documented;

c) conservation, quality, and replicability of the underlying data, the versioning of algorithms and documentation;

d) transparency, accuracy, explainability, and accountability of the models, ensured by a structured development and validation process carried out through appropriate IT management tools, well documented to support the internal audit and supervisory evaluation processes, and by means of the deployment of user-friendly GUIs and training support to the business units, in particular for origination purposes;

e) IT security, robustness, and safety, thanks to the IT system in use which ensures integrated and documented governance of the model life cycle, auditability of datasets, processes, and decisions taken during the development and validation phases, analysis of results, and operational continuity by virtue of business continuity and disaster recovery.

Compliance with the principles highlighted above acts also as a safeguard to the principles of sustainability as well as a mitigation of reputational risks for the illimity Group.

The illimity Group undertakes to make every effort to comply with the guidelines defined and developed from time to time by national and international regulatory bodies involved in AI, as well as those issued by the banking authorities with regard to this topic.

4 CLASSIFICATION AND MANAGEMENT MODEL

With reference to the classification and treatment of Artificial Intelligence models according to a risk-based approach, the Group undertakes to apply the proposed European Union Regulation that establishes harmonized rules on artificial intelligence (so-called Law-Act on Artificial Intelligence) and changes some legislative acts of the union.

With reference to the definition of the Artificial Intelligence algorithms, the Group adopts the definition of the proposed regulation, specifying that - in line with the opinion formulated by the European Central Bank – are excluded those models that are either deterministic or based on analytical functional forms between model's features and targets. In fact, it is understood that the Group intends to comply in any case with the principles illustrated in paragraph 3 for any model based on data and implemented through IT algorithms. However, the Group believes that the need for specific ethics, governance, and control requirements is necessary only for AI models in the strict sense, for which the potential elements of discrimination and bias might be difficult to identify, given the complexity of their explainability.

By way of example, linear or logistic regressions are therefore not the subject of this policy, as well as deterministic expert systems. In summary, this policy is applied to AI models that implement:

1. machine learning approaches, including supervised, unsupervised, and reinforcement learning, using a wide range of methods including deep learning;

2. logic and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inferential and deductive engines, (symbolic) reasoning, and expert systems;

3. statistical approaches, Bayesian estimation, search and optimization methods;

4. in any case, are excluded those approaches for which either the function that links the features to the relative targets is known in analytic form or those that are based on deterministic rules.

In particular, in accordance with Title II of this legislative proposal, illimity adopts the list of prohibited artificial intelligence practices, including in particular those concerning the potential manipulation of people.

The following AI models are defined as high risk under this policy, and the list below is kept updated to take into account new regulatory guidelines or new practices or techniques that may emerge from time to time. Reference is made to the list contained in the proposed Regulation, specifying if the scope is not applicable to the Group ("NOT APPLICABLE"), and enriching the list of any new inclusions ("ADDED"), including e.g. the ones as suggested by the European Central Bank:

1. Biometric identification and categorization of natural persons:

    a. AI systems intended to be used for "real-time" and "post" remote biometric identification of natural persons.

2. [NOT APPLICABLE] Management and operation of critical infrastructure:

    a. AI systems intended to be used as safety components in the management and operation of road traffic and the supply of water, gas, heating, and electricity.

3. [NOT APPLICABLE] Education and vocational training:

    a. AI systems intended to be used for the purpose of determining access or assigning natural persons to educational and vocational training institutions;

    b. AI systems intended to be used for the purpose of assessing students in educational and vocational training institutions and for assessing participants in tests commonly required for admission to educational institutions.

4. Employment, workers management and access to self-employment:

    a. AI systems intended to be used for recruitment or selection of natural persons, notably for advertising vacancies, screening or filtering applications, evaluating candidates in the course of interviews or tests;

    b. AI intended to be used for making decisions on promotion and termination of work-related contractual relationships, for task allocation and for monitoring and evaluating performance and behavior of persons in such relationships.

5. Access to and enjoyment of essential private services and public services and benefits:

    a. [NOT APPLICABLE] AI systems intended to be used by public authorities or on behalf of public authorities to evaluate the eligibility of natural persons for public assistance benefits and services, as well as to grant, reduce, revoke, or reclaim such benefits and services;

    b. AI systems intended to be used to evaluate the creditworthiness of natural persons or establish their credit score, with the exception of AI systems put into service by small scale suppliers for their own use;

    c. [NOT APPLICABLE] AI systems intended to be used to dispatch, or to establish priority in the dispatching of emergency first response services, including by firefighters and medical aid;

    d. [ADDED] AI systems that link sales, transactions, and performance data to assess conduct risk;

    e. [ADDED] AI systems aimed at real-time monitoring of payments, or profiling customers or transactions, for the purpose of preventing money laundering and terrorist financing.

6. [NOT APPLICABLE] Law enforcement:

    a. AI systems intended to be used by law enforcement authorities for making individual risk assessments of natural persons in order to assess the risk of a natural person for offending or reoffending or the risk for potential victims of criminal offences;

    b. AI systems intended to be used by law enforcement authorities as polygraphs and similar tools or to detect the emotional state of a natural person;

    c. AI systems intended to be used by law enforcement authorities to detect deep fakes as referred to in article 52(3);

    d. AI systems intended to be used by law enforcement authorities for evaluation of the reliability of evidence in the course of investigation or prosecution of criminal offences;

    e. AI systems intended to be used by law enforcement authorities for predicting the occurrence or reoccurrence of an actual or potential criminal offence based on profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680 or assessing personality traits and characteristics or past criminal behaviour of natural persons or groups;

    f. AI systems intended to be used by law enforcement authorities for profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680 in the course of detection, investigation or prosecution of criminal offences;

    g. AI systems intended to be used for crime analytics regarding natural persons, allowing law enforcement authorities to search complex related and unrelated large data sets available in different data sources or in different data formats in order to identify unknown patterns or discover hidden relationships in the data.

7. [NOT APPLICABLE] Migration, asylum, and border control management:

a. AI systems intended to be used by competent public authorities as polygraphs and similar tools or to detect the emotional state of a natural person;

b. AI systems intended to be used by competent public authorities to assess a risk, including a security risk, a risk of irregular immigration, or a health risk, posed by a natural person who intends to enter or has entered into the territory of a Member State;

c. AI systems intended to be used by competent public authorities for the verification of the authenticity of travel documents and supporting documentation of natural persons and detect non-authentic documents by checking their security features;

d. AI systems intended to assist competent public authorities for the examination of applications for asylum, visa and residence permits and associated complaints with regard to the eligibility of the natural persons applying for a status.

8. [NOT APPLICABLE] Administration of justice and democratic processes:

a. AI systems intended to assist a judicial authority in researching and interpreting facts and law and in applying the law to a concrete set of facts.

The use of high-risk AI models by the Group is limited, and, as far as possible, confined to internal use and to the controls of first and second-level risks. Its monitoring is implemented in the Risk Appetite Framework (as part of the Risk Appetite Statement) in the context of which zero or minimum level of risk appetite is defined. In any case, the possible adoption of a high-risk AI model is equivalent to a Significant Risk Transaction (so-called SRT, subject to approval by the Board of Directors after hearing the opinion of the Risk Committee, on the basis of a proposal accompanied by risk opinion by the second level control functions, including conformity assessments).

Also for the purpose of monitoring the adoption of the so-called high-risk artificial intelligence systems applied to individuals, the Group undertakes to create and manage an internal catalog relating to all the AI models used (developed internally or by external suppliers) which lists characteristics and purposes, illustrates the protection of the principles adopted by the Group, as well as contains a risk assessment by the first and second level functions, including compliance assessments for high-risk models.

Where applicable, the Group requires its suppliers to comply with the principles outlined in this Policy in Chapter 2, by accepting the Sustainable Supply Chain Policy.

5 RELATED REGULATION

RELATED INTERNALE REGULATION

Risk Management Policy
Policy about Internal Risk Models Governance
Policy about the Significant Risk Transactions (SRT)
RAF Policy: Risk Appetite Statement
IT Security Policy
Sustainable Supply Chain Policy
Illimity Way

RELATED EXTERNAL GUIDELINES AND REGULATION

Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: Artificial Intelligence for Europe
Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (GDPR)
OECD Recommendation of the Council on OECD Legal Instruments Artificial Intelligence
OECD AI Principles
EU Ethics guidelines for trustworthy AI
Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts
Opinion of the European Central Bank of 29 December 2021 on a proposal for a regulation laying down harmonised rules on Artificial Intelligence