Global Policy

General principles on Artificial Intelligence

FB 032_2024

Approving Function	Board of Directors	**Date** July 2024	
Proposer Function	ICT & Security Office Department (CIO)		

MASTER RECORDS

Owner	ICT & Security Office Department (CIO)		
Process Tree	Process Type: Operations and business support - MG: Human Resources and Infrastructure Management - MP: Information System Management - EP: ICT Architecture Management - SP: Artificial Intelligence (AI)		
Contacts	***Clarification of the contents of this document***	Unit: ICT & Security Governance e-mail: ICT_SecGov@fineco.it	
	Operational support	ICT_SecGov@fineco.it	
Holding Company departments involved in the information sharing process	CRO Department Compliance Department Data Protection Officer (DPO) Procurement Office Organizzazione e Operations Banca Department CFO – Sostenibilità Department Global Business Department Legal & Corporate Affairs		
Holding Company certification by area of responsibility	Compliance Department		
Entities involved in the sharing process			
Recipient entity (minimum perimeter)[1]	**Direct Legal Entities**	**Indirect Legal Entities**	**Other guidelines**
	Fineco Asset Management DAC (FAM)		

[1] In addition to the Entities indicated above, each Entity may distribute the Global Rule to its Legal Entities

Regulations replaced/revised and main changes made

Regulations replaced/ revised	Date regulation replaced/ revised	Reason for/summary of key amendments	Type of change[2]
FB 032_2024	Luglio 2024	The reference to the AI Act has been updated following its publication in the Official Gazette on the 12th of July.	Minor Change
-			First Release

Holding Local Regulations

Title	Regulation number	Brief explanation of the connection
Internal Regulation	-	The document defines corporate roles and responsibilities in accordance with the current organizational structure.
Document of Bodies and Functions with Control Tasks	-	The document is dedicated to control bodies and provides detailed descriptions of their duties and related responsibilities.

Related Group Regulation

Title	Regulation number	Brief explanation of the connection
Global Policy on Major Significant Transactions	FB 049_2021	The Global Policy establishes principles and rules for the management, identification, and evaluation of Major Significant Transactions within FinecoBank Group, to which the adoption of a high-risk AI model would be comparable.
Global Policy Risk Appetite Framework	FB 029_2022	The Global Policy defines the guidelines and governance of the FinecoBank Group related to the Risk Appetite Framework (RAF).
Global Policy General Security Policy	FB 005_2021	It describes the guidelines to be followed to ensure that each IT resource is protected, in terms of

[2] Minor change: approval of Target Entities not required
First release/Replacement: approval of Target Entities required

		confidentiality, integrity, availability, verifiability and accountability, appropriately and consistently throughout its life cycle.
Global Policy – Sustainability Policy	FB 002_2024	It governs the principles and procedures for managing sustainability in Fineco Group.
Global Policy Privacy	FB 076_2020	It transposes the provisions introduced by the General Data Protection Regulation (EU) 2016/679 to define minimum requirements on data protection topics.
Code of Integrity, Code of Conduct, and Compliance Culture	FB 021_2023	The Global Policy defines the principles and values to which the Group Legal Entities want to conform their operations, the set of rights, duties and responsibilities that they assume towards all stakeholders, and are part of the Group's corporate culture.

Index

1. INTRODUCTION

1.1. Scope of Application

FinecoBank SpA, as the Holding Company - in compliance with current laws and regulations[3] and in coherence with the group managerial coordination system defined by the Group Managerial Golden Rules - issues guidelines, in the interest of Group stability and with the aim to fully exercise its management and coordination role.

This document integrates the Group regulations. It is directly applicable to the Holding Company[4] and is addressed to the Legal Entities.

As provided for in the Global Policy about Group Management of Regulations, this document shall be adopted in accordance with the requirements and regulations in force locally; in the event of any conflict between this Global Rule (hereinafter also GR) and applicable local law (or in the event of greater restrictions), the latter shall prevail.

After approval by the competent bodies of Fineco, as the Holding Company, it transmits the GR to the recipient Entities for approval by their respective Corporate Bodies and monitors its correct and timely implementation, leveraging its internal functions as identified from time to time.

Therefore, the Group companies are required to promptly initiate - after appropriate assessment and approval by their competent bodies - the necessary activities aimed at the correct application of this document.

If the Legal Entity considers:

- this Global Rule is not applicable, or
- it is necessary to make changes/derogations to the provisions contained in this Global Rule,

for the purposes of compliance with local regulations (if more restrictive) or due to organisational and operational constraints, the Entity, in accordance with the provisions of the Group regulations in force (Management of Group Regulations), must submit a request for a Non Binding Opinion (NBO) to the ICT & Security Office (CIO) of the Holding Company.

1.2. Document purpose

The purpose of this Global Policy (hereinafter also referred to as Policy or GP) is to transpose, from time to time and consistently with the characteristics of its business model, the voluntary indications on ethical profiles defined at European Union and Organization for Economic Co-operation and Development (OECD) level, with reference to the governance of AI (Artificial Intelligence) models used by FinecoBank Group. The Group also commits to implement these guidelines in compliance with Information Security rules.

In particular, referring to the European Commission's Communication of April 21, 2021 on Artificial Intelligence for Europe, and considering the General Data Protection Regulation (GDPR), as well as taking into account the Regulation establishing harmonized rules on artificial intelligence (the AI

[3] Internal and external regulations in force at the issue date of this document; subsequent updates, where applicable from time to time.

[4] In the event of any discrepancy between the Holding Company's Responsibilities set out in these rules and those set out in the Rules of Corporate Bodies, Articles of Association, Internal Rules, Delegated Powers of FinecoBank in force from time to time, the latter shall always prevail.

Act), the FinecoBank Group acknowledges the importance of addressing challenges related to the use of AI and the ethical aspects arising from it. In this regard, the Group continuously monitors regulatory developments, including guidelines, for timely incorporation and adaptation of its internal regulations where applicable and deemed appropriate.

Furthermore, also considering the OECD Council Recommendation on Artificial Intelligence, the following chapter sets out the principles and guidelines by which the Group is guided in its approach to this topic, with reference to model governance and information security.

For AI systems served by Group Legal Entities in their capacity as financial institutions, the governance requirements, arrangements or internal processes established under EU financial services law apply, subject to the provisions of the Artificial Intelligence Act to which reference is made.

1.3. External regulatory framework

- Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized rules on artificial intelligence
- European Commission Communication to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions promoting a European approach to artificial intelligence (COM(2021) 205 final)
- Common Declarations of the European Parliament, of the Council, of the European Commission, European Declaration on Digital Rights and Principles for the Digital Decade (2023/C 23/01)
- Opinion of the European Central Bank of 29 December 2021 on a proposal for a regulation establishing harmonized rules on artificial intelligence
- Opinion of the European Economic and Social Committee of 22 September 2021 (COM(2021) 188 final)
- Principles for trustworthy AI defined by the OECD Observatory initially adopted in 2019 and updated in May 2024;
- Ethical guidelines for trustworthy AI - High-Level Expert Group on Artificial Intelligence (AI HLEG) – April 8, 2019.
- ESMA Statement on the use of Artificial Intelligence (AI) in the provision of retail investment services - 30/05/2024 (ESMA35-335435667-5924)
- OECD Council Recommendation on Artificial Intelligence (OECD/LEGAL/0449)
- General Data Protection Regulation (EU) 2016/679 (hereinafter also referred to as "GDPR").
- Legislative Decree 30 June 2003, No. 196, known as the "Personal Data Protection Code."

1.4. Glossary and Definitions

Key words	Definition
Holding Company	FinecoBank S.p.A. (hereinafter also “FinecoBank”, “Fineco” or “Bank”)

Legal Entity	The Company directly or indirectly owned by FinecoBank S.p.A. (hereinafter also "Subsidiary Entity", or "Subsidiary" or in brief "LE")
Group Companies	Companies of the FinecoBank Group, which is the Holding Company FinecoBank and its Subsidiaries
Group	FinecoBank Group, consisting of FinecoBank S.p.A. and Group Companies (hereinafter also “Fineco Group”)
Artificial Intelligence (AI) system	A machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, contents, recommendations, or decisions that can influence physical or virtual environments.
First and second level controls	As defined in the Document of Bodies and Functions with Control Tasks, first-level controls pertain to the execution of individual work activities and are implemented based on executive procedures specifically prepared according to internal regulations. The operational structures are primarily responsible for the risk management process. Second-level controls aim mainly to ensure the correct implementation of the risk management process. These controls are assigned to the second-level corporate control functions based on their competence.
Personal data	Any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.
High-risk AI model	AI models that, due to their scope of application, pose significant potential risks to the health and safety or fundamental rights of individuals, and for which a robust methodology for managing such risks must therefore be implemented.
Major Significant Transaction (MST)	Transactions, carried out by the Holding Company or its Legal Entities, that have the potential to significantly alter the business context of the Group, leading to exceeding relevant thresholds of Risk Appetite (Warning Threshold, Risk Tolerance, and Risk Capacity).
OECD	Organisation for Economic Cooperation and Development

ICT and security risk	The risk of incurring losses due to breaches of confidentiality, inadequate integrity of systems and data, inadequacy or unavailability of systems and data, or inability to replace information technology (IT) within reasonable time and cost limits in the event of changes in external context or business requirements (agility), as well as security risks arising from inadequate or incorrect internal processes or external events, including cyber-attacks or inadequate physical security. In the integrated representation of enterprise risks for prudential purposes (ICAAP), this type of risk is considered, depending on specific aspects, among operational, reputational, and strategic risks.
Operational risk	Operational risk is defined by Article 4 of Regulation 575/2013 (CRR) as "the risk of losses resulting from inadequate or failed internal processes, systems, human resources, or from external events, including legal risk." The scope of operational risks described includes IT risk, which is the risk of incurring economic losses, reputational damage, and market share declines related to the use of Information and Communication Technology (ICT).
Reputational risk	Reputational risk is the current or prospective risk of a decline in earnings or capital resulting from a negative perception of the Group's image by customers, employees, counterparties, bank shareholders, investors, or regulators. Reputational risks can be considered as a secondary effect of all other categories of risk, such as credit risk, market risk, operational risk, and liquidity risk. Exposure to reputational risk is therefore induced by other types of risk: identifying this exposure involves analyzing exposure to original risks to identify what is "sensitive" in terms of reputational risk.
Systemic Risk	The "systemic risk at Union level" refers to the possibility that the use of AI could have a significant impact on the internal market due to its scope and with real or reasonably foreseeable negative effects on public health, safety, fundamental rights, or society as a whole, which can propagate on a large scale throughout the value chain. For example, if a widespread malfunction of an autonomous driving application were to occur, it could cause large-scale traffic accidents, thereby influencing the entire urban mobility system.
Internal AI Catalog	Internal AI Catalog (also register) listing all AI models used (developed internally or by external providers), detailing their characteristics and purposes, illustrating adherence to Group adopted principles, as well as containing risk assessments by first and second-level functions including compliance evaluations for high-risk models.

Acronym	Definition
ICT	Information & Communication Technology
AI	Artificial Intelligence
OECD	Organisation for Economic Cooperation and Development
HLEG	High level Expert Group
FLOPS	Floating point operations per second
GPAI	General Purpose AI
LLM	Large Language Models

2. GENERAL PRINCIPLES

For the purposes of this document, the FinecoBank Group is committed to complying with the application of the best standards and best practices about Artificial Intelligence, developing, distributing and using its AI models in compliance with the Regulation of the European Parliament, Artificial Intelligence Act (AI Act), and in line with the principles defined by the OECD Observatory and the European Commission's Ethical Guidelines for Trustworthy AI. Therefore the Group is committed to respect the following principles and guidelines:

a) **Sustainable development and well-being**, through models that are more efficient compared to traditional ones, as they are able to ensure better risk management and control, contributing to the strengthening of the mechanisms for the proper operation of markets and, more generally, of the global economy;

b) **centrality of the human factor**, which maintains a crucial role in the development and validation phases of the models, through the involvement of the appropriate stakeholders consistent with the peculiarities of the models themselves, as well as in the downstream control phases, through appropriately documented final processes;

c) **transparency, accuracy and explicability of the models**, through the implementation of: a structured development and validation process, governed by IT tools according to best practice and adequately documented; user-friendly IT interfaces and training support for their use, in particular to ensure that the output of the model is consistent with what was defined in the design phase;

d) **IT security, robustness, and safety**, thanks to the ICT systems in use that ensure integrated and documented governance of the life cycle of models (including the traceability of the datasets used), of the related processes and decisions taken during their development and validation, and finally the analysis of the results obtained.

FinecoBank Group adopts a risk-based approach consistent with the Regulation of the European Parliament, ensuring compliance with the following additional requirements for high-risk AI systems while always considering the aforementioned principles:

a) preservation, quality, accuracy, and replicability of the data underlying these models, and version control of the algorithms and supporting documentation.
b) resilience with respect to errors, failures, or inconsistencies that may occur within the system or the environment in which it operates, particularly due to their interaction with individuals or other systems, as well as resilience against attempts by unauthorized third parties to alter the use or performance of the high-risk AI system.

Compliance with the aforementioned principles also serves as a guarantee to uphold the Group's sustainability principles, as well as to mitigate the Group's exposure to reputational risks for the FinecoBank Group.
The Group commits to paying particular attention to the aspects listed below in accordance with the guidelines/regulations issued regarding AI:

- **Transparency and accountability**, through clear and adequate information whenever interaction with AI systems is expected, also specifying the type of data collected and how it is used by the systems. The AI systems used by the Group maintain a strong focus on humans as such, acting as supporting tools to ensure they always maintain a central role in all decision-making processes. Additionally, the utilized systems are characterized by a strong innovative component, aimed at continuously improving the customer experience to make it as smooth and intuitive as possible across all channels. Customer satisfaction in terms of user experience in using the services offered by the Bank, as well as their reliability and security, represents a key element for the Group;

- **Ethics and fairness** – The FinecoBank Group is committed to developing AI systems in an ethical and fair manner in order to increase trust on the part of the users of such systems. It is important to ensure that the results obtained from such systems steer all individuals in their decisions in a fair and non-discriminatory manner, and that the data used by the systems are, where possible, adequately anonymised or pseudo-anonymised. Furthermore, the Group, through the structures identified from time to time during the implementation of this GP, ensures adequate human oversight to control the operation and use of the AI systems; in fact, all experts involved in the development and deployment of the AI systems are subject to the Group's Code of Conduct, which includes explicit provisions for fair treatment, against discrimination and prejudice.
  The FinecoBank Group is committed to mitigating any digital divide that may occur due to different access to Artificial Intelligence-based technologies, also by raising awareness among its partners and suppliers.
- **Privacy and security** – Particular attention is always paid to these topics since the design phase of AI systems, as enabling factors for the correct definition of the solutions offered, also taking advantage of any opportunities arising from the evolution of the regulatory context in which the Group operates, in order to ensure full security for the users of AI systems, while guaranteeing ease of use. The context is characterised by increasing digital complexity and information security has become crucial for the banking sector.
  The steps taken to improve IT security management contribute to mitigating the Group's exposure to operational and reputational risks as well as vulnerabilities and evolving threats. In fact, the necessary security measures are taken to mitigate the risks inherent to the services offered, applying the best market practices in the field of security and ensuring the unity within the Group of the ICT risk management vision, as well as the uniformity of application of information system standards.
- **Human rights, diversity and inclusiveness** – The FinecoBank Group recognises the importance of respect for human rights, and its essentiality for proper business conduct. Furthermore, the Group bases its activities on guaranteeing and promoting respect for all human rights, defining an inclusive approach and ensuring compliance with the relevant national and international regulations and standards. The Group's commitment is aimed at promoting diversity and inclusiveness in order to enable the creation of a corporate culture that guarantees a working environment free from any form of discrimination in respect of human dignity. The commitment to human rights also concerns the supply chain, with the aim of minimising the risks of rights violations; to this end, the Group has made the assessment of suppliers more efficient in relation to social and environmental impacts, evaluating the characteristics of the supply chain also in terms of respect for and protection of human rights. This commitment is also demonstrated by the adoption of best practices in the AI area.
- **Maximising the benefits of AI while maintaining the central role of the human factor**: consistent with its digital nature, the FinecoBank Group is determined to invest more and more in digital business while keeping the human factor at the heart of its business as a critical success factor.
  In a context characterised by increasing digital complexity, it is risky to rely on technology only, and, therefore, the human factor continues to represent one of the Fineco Group's most important protection rings, and it is essential to continue to ensure that there is awareness and monitoring of possible threats, both from clients and from employees and management, in order to be able to recognise them and be able to react appropriately.

Fineco also recognises that the use of AI can play a major role in the pursuit of the Group's objectives of innovation and environmental and social sustainability throughout its value chain.

The use of AI models can in fact contribute to reducing the environmental impact of activities, e.g. promoting a more sustainable use of resources, by monitoring and analysing data and AI-managed processes. Data produced and managed by AI can also be used to understand processes related to climate change and consequently develop new models that can improve the management of environmental risks.

From a social point of view, the respect for the principles of equity, diversity and non-discrimination in the design and application of AI fosters the reduction of inequalities, helping to promote and improve accessibility and inclusion.

3. CLASSIFICATION AND MANAGEMENT OF MODELS

With regard to the classification and treatment of Artificial Intelligence models according to a risk-based approach, the FinecoBank Group is committed to implementing the European Union Regulation, Artificial Intelligence Act (AI Act), which establishes harmonised rules on artificial intelligence and amends some previous legislation acts issued by the European Union.

With reference to the definition of Artificial Intelligence algorithms, the Group follows the Regulation and - in line with the advice of the European Central Bank - adopts a 'risk-based' approach to the use of such algorithms. This approach provides that a higher level of risk is matched by stricter rules of use.

In particular, the Group applies the classification model divided into: i) unacceptable risk; ii) high risk; iii) limited risk; and iv) minimal risk.

The Group intends to respect this classification and undertakes to adopt the following practices, based on the risk classes:

AI practices for unacceptable risk

Do not implement Artificial Intelligence practices that present an unacceptable risk to the security, livelihood, and rights of people. In particular, the following are prohibited:

- Systems exploiting people's vulnerability through subliminal, manipulative and deceptive techniques;
- Systems of biometric categorisation of individuals to deduce or infer ethnicity, political opinions, trade union membership, religious beliefs and sexual orientation;
- Biometric identification systems (facial recognition) in real time in publicly accessible spaces;
- Emotion recognition systems used in the workplace, except for medical or security reasons;
- The untargeted extraction (scraping) of facial images from the internet or closed-circuit television cameras for the creation or expansion of databases;
- Systems that enable 'social scoring' by classifying or rating people according to their social behaviour or personal characteristics.

AI practices for high-risk systems

Implement systems falling into this category by complying with all the requirements defined in the AI Act, in particular by demonstrating that each system complies with the mandatory requirements for reliable AI (e.g. data quality, documentation, data and model traceability, human oversight, accuracy, cybersecurity and robustness).

Systems must be technically robust to ensure that the technology is suitable for the purpose and that results, in terms of accuracy and false positives/negatives, do not impact disproportionately (bias) on protected groups (e.g. by ethnic origin, gender, age, etc.). The systems must also be trained and tested with data sets that are sufficiently representative of the Group's data to minimise the risk of incorporating unfair biases, which, if present, must be resolved by appropriate corrections and mitigations. The data used for training and testing the algorithm must also be traceable and verifiable, ensuring that appropriate documentation is kept in compliance with the legislation applicable from time to time on the processing of personal data, including Regulation (EU) 2016/679.

Finally, the Group commits to conducting an impact assessment on the fundamental rights of individuals, which consists of a description of the processes in which the IA system will be used, the time period and frequencies in which the system is intended to be used, the categories of individuals and groups that may be affected by its use, the specific risks of harm that may affect the categories of individuals and groups that will use it, and a description of the human oversight measures and the measures to be taken if the risks materialise.

For high-risk systems, reference is made to the list contained in the AI Act (Annex III), specifying if the scope does not apply (**OOS-out of scope**) to the Group:

- Biometric identification/categorisation systems, protected by Article 9(1) of Regulation (EU) 2016/679, which excludes AI systems used for remote authentication to access Group services by customers, that are not considered high risk;
- Systems related to employment assessment, aimed at optimising the management of workers and access to self-employment (e.g. publishing targeted job advertisements, analysing and filtering applications and assess candidates);
- Systems aimed at assessing the creditworthiness of individuals, assessing financial risks, as well as pricing in relation to life and health insurance;
- Systems aimed at Anti-Money Laundering (AML) activities, used for the purpose of preventing, identifying, investigating and pursuing illegal activities;
- (**OOS**) Systems used as safety components in the management and operation of critical digital infrastructure, road traffic and the supply of water, gas, heating and electricity;
- (**OOS**) Systems aimed at determining access, admission or assignment to educational and professional training institutions (e.g. for assessing learning outcomes and guiding the learning process and monitoring dishonest behaviours);
- (**OOS**) Systems used to determine access to essential public and private services and benefits (such as health care);
- (**OOS**) Systems used in law enforcement, migration management, asylum and border control, administration of justice, as well as in the conduct of democratic processes and for the evaluation and classification of emergency calls.

An IA system listed in Annex III is always considered high-risk if it performs profiling of natural person.

Limited risk systems

Implement, as defined by the AI Act, transparency mechanisms for AI systems related to this category. In particular, the Group is committed to introducing communication and transparency mechanisms aimed at informing customers about the direct use of AI-based systems. This will allow customers to make informed choices regarding the continued use of limited-risk AI services. FinecoBank is committed to making it clearly recognizable to customers when they are interacting with an AI system, allowing them to consciously decide whether to continue its use. The Group is committed to ensuring that AI-generated content in the form of text, images, and videos is clearly identifiable.

Minimum risk systems

Comply with the AI Act for this category, subject to alignment with the Group's Code of Conduct. This category includes AI systems used for automatic document classification, automatic extraction of structured data from unstructured sources, process automation, automatic document review (for tone, style and language, Group branding), automatic discovery of anomalies, smart solutions for document management (indexing, searching, text and speech processing, entity liking, document translation), i.e. all those AI systems that do not influence people's decisions or interests or offer secondary support to activities carried out personally by people.

In addition to the risk-based approach, the Group follows the 2019 Ethical Guidelines for Trustworthy AI, developed by the independent *High Level Expert Group on Artificial Intelligence* (AI HLEG) appointed by the European Commission. In these guidelines, the AI HLEG has developed seven non-binding ethical principles for AI, which are intended to ensure that AI is reliable and ethical. The seven principles are: human intervention and oversight; technical robustness and security; privacy

and data governance; transparency; diversity, non-discrimination and fairness; social and environmental well-being and accountability.

With regard to *General Purpose AI* (GPAI) systems, such as *Foundational Models* and *Large Language Models* (LLM), i.e. for models with more than 10^25 FLOPS, the Group undertakes to comply with the requirements of the AI Act, which means that all these models will fall under the risk categorisation of the AI system in which they will be marketed. If they are used for research purposes or internal experiments, they will not fall under the high-risk systems categorisation. In addition, the Group undertakes, in the event of GPAI systems being placed on the market, to apply the recommendations relating to *systemic risks*.

The risk appetite for the use of high-risk AI models is established within the Risk Appetite Framework (as part of the Risk Appetite Statement). The use of high-risk AI models by the Group is limited and, as far as possible, confined to internal use and subject to first and second-level control measures in line with the Bank's internal control and risk management system. In this regard, the potential adoption of a high-risk AI model is equated to a Major Significant Transaction (whose evaluation and approval follow the process defined in the Global Policy on Major Significant Transactions, to which reference is made for quick reference).

In order to monitor the adoption of so-called high-risk artificial intelligence systems in relation to individuals, the Group is committed to creating and managing an internal catalog of all AI models used (developed internally or by external providers). This catalogue will list the characteristics and purposes of each model, illustrate the adherence to principles adopted by the Group, and include a risk assessment carried out by first and second-level functions, including compliance evaluations for high-risk models.

4. Roles and Responsibilities

4.1 Responsibilities of the Holding Company

In order to effectively govern AI and ensure that it is used in a safe and responsible manner, in compliance with the reference regulations, it is essential to define an organisational model, which provides for the definition and assignment of roles and responsibilities within the Group and its companies.

The Group is committed, through the functions involved (by way of example but not limited to: Global Business, Sustainability, DPO, risk management, compliance, legal, BPR, ICT, Security, Human Resources, etc.), to carry out an assessment, by area of competence, of project initiatives that envisage the use of AI systems through internal demand and project management processes. By way of example:

- DPO, consistent with its current attributions, monitors that the AI application does not prejudice compliance with the legislation applicable at the time governing the processing of personal data;
- Legal, in line with its attributions and competences, for the AI scope, ensures compliance with applicable regulations, such as, but not limited to, intellectual property, licensing agreements and the definition of contracts with suppliers, customers and more generally with third parties;
- Sustainability, consistent with its attributions, for the AI scope, ensures compliance with the principles of ethics and fairness, as well as respect for environmental resources.

In addition, Fineco, with reference to the Holding Company, integrates the Artificial Intelligence principles into its governance system, assigning, or confirming where already in place, responsibilities to governing bodies and corporate functions, as outlined below:

- the Board of Directors, in its capacity as the body with strategic supervisory functions, approves the strategic policies on Artificial Intelligence, preliminarily supported by the endoconsiliar committees, such as, principally, the Risks and Related Parties Committee and the Corporate Governance and Environmental and Social Sustainability Committee, each within the scope of its competence;
- the Chief Executive Officer and General Manager, in his capacity as Body with Management Function, has the task, also in the AI area, consistent with his current attributions, of ensuring the completeness, adequacy, functionality and reliability of the information system; in addition, he draws up the action plans containing the measures to be adopted to achieve the ICT strategy objectives, monitors and measures their effectiveness, and periodically reviews them, reporting to the Board of Directors; approves, at least once a year, the operational plan of ICT initiatives, verifying their consistency with corporate strategies and the information and automation needs of business areas; ensures the definition of roles and related responsibilities for the ICT function and for ICT and security risk management; approves the procedures and processes for managing ICT operations concerning resources and services that have not been outsourced, guaranteeing the effectiveness and efficiency of the system as well as its overall completeness and consistency;
- ICT & Security Office (CIO): consistently with its current duties, for the AI scope, ensures the preparation, adoption and management of the internal ICT and Security regulations, supports the Chief Executive Officer and General Manager in defining (and updating as necessary) the Action Plans for subsequent approval by the Board of Directors, containing the measures to

be adopted to implement the ICT strategy; ensures the preparation of the operational plan relating to IT initiatives, verifying its consistency with corporate strategies; submits the same plan for approval to the CEO and General Manager; prepares and oversees the adoption of policies and guidelines on Artificial Intelligence;

- Outsourcing Management: is responsible for coordinating internal information flows aimed at ensuring that the Bank's Corporate Bodies and Corporate Control Functions have a correct and complete assessment of the Bank's exposure to risks arising from ICT services provided by third parties and outsourcing agreements;
- Compliance, in line with its attributions, for the AI scope, verifies that internal procedures and processes are adequate to prevent the risk of non-compliance in the context of AI, including aspects relating to the processing of personal data, IT security, also by measuring the risk itself;
- Risk Management, consistent with its responsibilities, contributes for the AI scope in the analysis of ICT and security risks and is responsible for the monitoring and control of these risks, ensuring that they are identified, measured, assessed, managed and mitigated, monitored as well as reported and maintained within the limits of the bank's risk appetite;

It is allowed, if deemed appropriate, that specific working groups may be established, time by time identified, according to needs or events.

4.2 Responsibilities of the Subsidiaries

The Subsidiary Receiving Entity, with reference to the governance of the AI (Artificial Intelligence) models used by the Group and their implementation in compliance with Information Security rules, is responsible for:

- adopt and implement the rules and guidelines set out in this document, with reference to the governance of models and the security of information, consistently and in accordance with local particularities and relevant laws and regulations;
- collaborate in the sharing and knowledge of possible risks impacting the Group;
- provide periodical reporting on the correct compliance with the principles listed in this Global Policy.