Global Policy

Principi generali in tema di Artificial Intelligence

FB 032_2024

Funzione Approvante	Consiglio di Amministrazione	**Data** Luglio 2024	
Funzione Proponente	Direzione ICT & Security Office (CIO)		

Anagrafica

Owner	Direzione ICT & Security Office (CIO)		
Process Tree	Process Type: Operations e supporto al business - MG: Gestione delle risorse umane e delle infrastrutture - MP: Gestione del sistema informativo - EP: Gestione Architetture ICT - SP: Intelligenza Artificiale (AI)		
Contatti	***Chiarimenti sui contenuti del documento***	Struttura: ICT & Security Governance e-mail: ICT_SecGov@fineco.it	
	Assistenza operativa	ICT_SecGov@fineco.it	
Funzioni di Capogruppo coinvolte nel processo di condivisione	Direzione CRO Direzione Compliance Data Protection Officer (DPO) Procurement Office Direzione Organizzazione e Operations Banca Direzione CFO - Sostenibilità Direzione Global Business Direzione Legal & Corporate Affairs		
Certificazione in Capogruppo per profili di competenza	Direzione Compliance		
Entità coinvolte nel processo di condivisione			
Entità destinatarie (perimetro minimo)[1]	**Controllate dirette**	**Controllate indirette**	**Altre indicazioni**
	Fineco Asset Management DAC (FAM)		

[1] In aggiunta alle Entità indicate, ogni Entità può distribuire la *Global Rule* ad ulteriori proprie controllate

Normative sostituite/revisionate e principali cambiamenti apportati

Normativa sostituita/ revisionata	**Data normativa sostituita/ revisionata**	**Razionale/Riassunto delle principali modifiche**	**Tipo modifica[2]**
FB 032_2024	Luglio 2024	Aggiornamento della reference all'AI Act a seguito della pubblicazione in Gazzetta Ufficiale in data 12 luglio 2024	Minor Change
-			Prima release

Normativa Locale della Capogruppo

Titolo	**Numero Rule**	**Breve spiegazione del legame**
Regolamento interno	-	Il documento declina i ruoli e le responsabilità aziendali, in linea con l'organigramma tempo per tempo in essere.
Documento degli organi e delle funzioni con compiti di controllo	-	Il documento è dedicato agli organi con funzione di controllo e ne descrive in dettaglio i compliti e le responsabilità correlate.

Normativa di Gruppo collegata

Titolo	**Numero Rule**	**Breve spiegazione del legame**
Global Policy Operazioni di Maggior Rilievo	FB 049_2021	La Global Policy definisce principi e regole per la gestione, l'identificazione e la valutazione delle Operazioni di Maggior Rilievo all'interno del Gruppo FinecoBank, alle quali è equiparabile l'eventuale adozione di un modello AI ad alto rischio
Global Policy Risk Appetite Framework	FB 029_2022	La Global Policy definisce le linee guida e la governance del Gruppo FinecoBank relative al Risk Appetite Framework (RAF).

[2] Modifica minor: approvazione Entità destinatarie non necessaria
Prima release / Sostituzione: approvazione Entità destinatarie necessaria

Global Policy General Security Policy	FB 005_2021	Descrive le linee guida da seguire volte a garantire a ciascuna risorsa informatica una protezione, in termini di riservatezza, integrità, disponibilità, verificabilità e accountability, appropriata e coerente lungo l'intero ciclo di vita.
Global Policy – Policy di Sostenibilità	FB 002_2024	Disciplina i principi e le modalità di gestione della Sostenibilità nel Gruppo Fineco.
Global Policy Privacy	FB 076_2020	Recepisce le disposizioni introdotte dal Regolamento Generale sulla protezione dei dati personali (UE) 2016/679 in modo da definire dei requisiti minimi su tematiche relative alla protezione dei dati.
Carta d'Integrità, Codice di Condotta e Compliance Culture	FB 021_2023	La Global Policy definisce i principi e i valori ai quali le Società del Gruppo vogliono conformare la propria operatività, l'insieme dei diritti, dei doveri e delle responsabilità che le stesse assumono nei confronti di tutti i portatori di interessi, e costituiscono patrimonio della cultura di impresa del Gruppo

Indice

1. INTRODUZIONE

1.1. Ambito di applicazione

FinecoBank S.p.A., in qualità di Capogruppo - in conformità alle leggi e regolamenti vigenti[3] ed in coerenza con il sistema di coordinamento manageriale di gruppo definito dalle Group Managerial Golden Rules - emette linee guida, nell'interesse della stabilità del Gruppo, allo scopo di esercitare compiutamente il proprio ruolo di gestione e coordinamento.

Il presente documento integra la normativa di Gruppo, è direttamente applicabile alla Capogruppo[4] ed è indirizzato alle Entità del Gruppo (Entità o Società) destinatarie.

Come previsto dalla Global Policy di Gestione della Normativa di Gruppo, il presente documento sarà adottato in conformità ai requisiti e alle normative vigenti localmente; in caso di qualsiasi conflitto tra codesta Global Rule (di seguito anche GR) e la legge locale applicabile (o in caso di maggiori restrizioni), quest'ultima prevale.

Dopo l'approvazione da parte degli organi deputati di Fineco, la stessa, in qualità di Capogruppo, trasmette la GR alle Entità destinatarie per l'approvazione da parte dei rispettivi Organi Societari e ne monitora la corretta e tempestiva implementazione anche avvalendosi delle sue funzioni interne di volta in volta indentificate.

Le Società del Gruppo sono pertanto tenute ad avviare tempestivamente – dopo l'opportuna valutazione ed approvazione da parte dei propri Organi competenti – le necessarie attività finalizzate alla corretta applicazione del presente documento.

Nel caso in cui la Società ritenesse:

- la presente Global Rule non applicabile, ovvero
- necessario apportare delle modifiche/deroghe alle previsioni contenute nella presente Global Rule,

ai fini della conformità con la normativa locale (se più restrittiva) o in ragione di vincoli di natura organizzativa ed operativa, la Società, ai sensi di quanto disposto dalla normativa di Gruppo vigente (Gestione della Normativa di Gruppo), dovrà formulare alla Direzione ICT & Security Office (ClO) di Capogruppo una richiesta di Non Binding Opinion (NBO).

1.2. Scopo del documento

La presente Global Policy (di seguito anche Policy o GP) ha l'obiettivo di recepire, tempo per tempo ed in coerenza con le caratteristiche del proprio modello di business, le indicazioni volontarie in materia di profili etici definite a livello di Unione Europea e di Organizzazione per la Cooperazione e lo Sviluppo Economico (OCSE), con riferimento al governo dei modelli AI (*Artificial Intelligence*) utilizzati dal Gruppo FinecoBank, che si impegna altresì ad implementare nel rispetto delle regole di Sicurezza delle Informazioni.

[3] Normative interne ed esterne vigenti alla data di emanazione del presente documento; successivi aggiornamenti, ove tempo per tempo applicabili.

[4] In caso divergenza tra le Responsabilità della Capogruppo indicate nella presente normativa e quelle riportate nel Regolamento degli Organi Aziendali, Statuto, Regolamento Interno, Poteri Delegati di FinecoBank tempo per tempo vigenti, prevalgono sempre queste ultime.

In particolare, facendo riferimento alla Comunicazione della Commissione Europea del 21 aprile 2021 sull'Intelligenza Artificiale per l'Europa, e tenendo in considerazione il Regolamento Generale sulla protezione dei dati (GDPR), nonché tenuto conto del Regolamento che stabilisce regole armonizzate sull'intelligenza artificiale (c.d. Regolamento sull'intelligenza artificiale) il Gruppo FinecoBank riconosce l'importanza di far fronte alle sfide legate all'utilizzo di AI e agli aspetti etici che ne derivano. A tal riguardo, il Gruppo FinecoBank monitora nel continuo gli sviluppi normativi, anche a livello regolamentare e di linee guida, per un puntuale e tempestivo recepimento e adeguamento della propria normativa interna, ove applicabile e ritenuto opportuno.

Inoltre, anche alla luce della Raccomandazione del Consiglio dell'OCSE sull'Intelligenza Artificiale, nel capitolo successivo sono circoscritti i principi e le linee guida alle quali il Gruppo FinecoBank si ispira nell'approccio a tale tematica, con riferimento alla *governance* dei modelli ed alla sicurezza delle informazioni.

Per i sistemi di IA messi in servizio da Società del Gruppo in qualità di istituto finanziario si applicano i requisiti in materia di governance, dispositivi o processi interni stabiliti a norma del diritto dell'Unione in materia di servizi finanziari, nel rispetto di quanto previsto dall'Artificial Intelligence Act a cui si rimanda.

1.3. Normativa esterna di riferimento

- Regolamento (UE) 2024/1689 del Parlamento Europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale
- Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni promuovere un approccio europeo all'intelligenza artificiale (COM(2021) 205 final)
- Dichiarazioni comuni del Parlamento Europeo, del Consiglio, della Commissione Europea, Dichiarazione europea sui diritti e i principi digitali per il decennio digitale (2023/C 23/01)
- Parere della Banca Centrale Europea del 29 dicembre 2021 relativo a una proposta di regolamento che stabilisce regole armonizzate sull'intelligenza artificiale (CON/2021/40)
- Parere del Comitato Economico e Sociale Europeo del 22 settembre 2021 [COM(2021) 188 final]
- Principles for trustworthy AI definiti dall'Osservatorio OCSE adottati inizialmente nel 2019 e aggiornati nel maggio 2024;
- Orientamenti etici per un'IA Affidabile - Gruppo di esperti ad alto livello sull'intelligenza artificiale (*High Level Expert Group on Artificial Intelligence,* AI HLEG) – 8 APRILE 2019
- Dichiarazione ESMA sull'utilizzo dell'Intelligenza Artificiale (IA) nella fornitura di servizi di investimento retail - 30/05/2024 (ESMA35-335435667-5924)
- Raccomandazione del Consiglio sull'intelligenza artificiale (OECD/LEGAL/0449)
- Regolamento Generale sulla protezione dei dati personali (UE) 2016/679 (qui di seguito anche "GDPR").
- D. Lgs. 30 giugno 2003, n.196 recante il "Codice in materia di protezione dei dati personali"

1.4. Glossario e Definizioni

Parola chiave	Definizione

Capogruppo	FinecoBank S.p.A. (di seguito anche “FinecoBank”, “Fineco” o “Banca”)
Società controllata del Gruppo	Entità direttamente o indirettamente controllata da FinecoBank S.p.A. (di seguito anche “Entità”, “Entità del Gruppo”, “Entità controllata”, “Entità consolidata”, “Società controllata”, “Società” o in breve “LE”)
Società del Gruppo	Società del Gruppo FinecoBank, intendendo la stessa Capogruppo FinecoBank e le sue Società controllate
Gruppo	Gruppo FinecoBank, composto da FinecoBank S.p.A. e dalle Società controllate del Gruppo (di seguito anche “Gruppo Fineco”)
Sistema di intelligenza artificiale (AI)	Un sistema automatizzato progettato per funzionare con diversi livelli di autonomia e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce, dall'input che riceve, come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali.
Controlli di primo e secondo livello	In base a quanto definito nel Documento degli Organi e delle Funzioni con Compiti di Controllo, i controlli di primo livello sono relativi allo svolgimento delle singole attività lavorative e sono posti in essere sulla base di procedure esecutive all’uopo predisposte sulla base di una apposita normativa interna. Le strutture operative sono le prime responsabili del processo di gestione dei rischi. I controlli di secondo livello hanno l’obiettivo di assicurare, tra l’altro, la corretta attuazione del processo di gestione dei rischi. Sono assegnati alle funzioni aziendali di controllo di secondo livello per competenza.
Dato personale	Qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale
Modello AI ad alto rischio	Modelli AI che, in forza del loro ambito di applicazione, pongono potenziali rischi significativi per la salute e la sicurezza o per i diritti fondamentali delle persone, e per i quali deve essere pertanto implementata una solida metodologia per la gestione di tali rischi
Operazione di Maggior Rilievo (OMR)	Transazioni, eseguite dalla Capogruppo o dalle sue Legal Entities, potenzialmente in grado di cambiare significativamente il contesto

	di business del Gruppo, portando ad uno sforamento delle soglie rilevanti del Risk Appetite (Warning Threshold, Risk Tolerance e Risk Capacity).
OCSE	Organizzazione per la cooperazione e lo sviluppo economico
Rischio ICT e di sicurezza	Il rischio di incorrere in perdite dovuto alla violazione della riservatezza, carente integrità dei sistemi e dei dati, inadeguatezza o indisponibilità dei sistemi e dei dati o incapacità di sostituire la tecnologia dell'informazione (IT) entro ragionevoli limiti di tempo e costi in caso di modifica dei requisiti del contesto esterno o dell'attività (agility), nonché i rischi di sicurezza derivanti da processi interni inadeguati o errati o da eventi esterni, inclusi gli attacchi informatici o un livello di sicurezza fisica inadeguato. Nella rappresentazione integrata dei rischi aziendali a fini prudenziali (ICAAP), tale tipologia di rischio è considerata, secondo gli specifici aspetti, tra i rischi operativi, reputazionali e strategici.
Rischio operativo	Il rischio operativo è definito dall'art. 4 del Regolamento 575/2013 (CRR) come "il rischio di perdite derivanti dalla inadeguatezza o dalla disfunzione di processi, risorse umane e sistemi interni, oppure da eventi esogeni, ivi compreso il rischio giuridico". Il perimetro dei rischi operativi così descritto comprende il rischio informatico, ossia il rischio di incorrere in perdite economiche, di reputazione e di quote di mercato in relazione all'utilizzo di tecnologia dell'informazione e della comunicazione (Information and Communication Technology – ICT).
Rischio reputazionale	Il rischio reputazionale è inteso come il rischio attuale o prospettico di flessione degli utili o del capitale derivante da una percezione negativa dell'immagine del Gruppo da parte di clienti, dipendenti, controparti, azionisti della banca, investitori o Regulators. I rischi di reputazione possono essere considerati come un effetto secondario di tutte le altre categorie di rischio, quali il rischio di credito, di mercato, operativo e di liquidità. L'esposizione al rischio reputazionale è dunque indotta da altre tipologie di rischio: individuare tale esposizione significa analizzare l'esposizione ai rischi originari per identificare ciò che è "sensibile" in termini di rischio reputazionale.
Rischio Sistemico	Il "rischio sistemico a livello di Unione" si riferisce alla possibilità che l'uso dell'IA possa avere un impatto significativo sul mercato interno a causa della sua portata e con effetti negativi reali o ragionevolmente prevedibili su salute pubblica, sicurezza, diritti fondamentali o sulla società nel suo insieme, che possono essere propagati su larga scala lungo tutta la catena del valore. Ad esempio, se un'applicazione di guida autonoma mal funzionasse

	su larga scala, potrebbe causare incidenti stradali su vasta scala, influenzando quindi l'intero sistema di mobilità urbana.
Catalogo interno AI	Catalogo interno (anche registro) relativo a tutti i modelli AI utilizzati (sviluppati internamente o da fornitori esterni) che elenchi caratteristiche e finalità, illustri il presidio dei principi adottati dal Gruppo, nonché contenga una valutazione di rischio da parte delle funzioni di primo e secondo livello, incluse le valutazioni di conformità per i modelli ad alto rischio.
Acronimo	**Definizione**
ICT	Information & Communication Technology
IA	Intelligenza Artificiale
OCSE	Organizzazione per la cooperazione e lo sviluppo economico
HLEG	High level Expert Group
FLOPS	Floating point operations per second
GPAI	General Purpose AI
LLM	Large Language Models

2. PRINCIPI GENERALI

Ai fini del presente documento, il Gruppo FinecoBank si impegna a rispettare l'applicazione dei migliori standard e *best practice* in materia di *Artificial Intelligence*, sviluppando, distribuendo ed utilizzando i propri modelli AI nel rispetto del Regolamento del Parlamento Europeo, Artificial Intelligence Act (AI Act), e in linea con i principi definiti dall'Osservatorio OCSE e con gli Orientamenti etici della Commissione europea per un'AI affidabile. Pertanto, in tale ottica, il Gruppo si impegna al rispetto dei seguenti principi e linee guida:

a) **sviluppo sostenibile e benessere**, tramite modelli più performanti rispetto a quelli tradizionali in quanto in grado di assicurare una migliore gestione e controllo dei rischi, contribuendo al rafforzamento dei meccanismi di corretto funzionamento dei mercati e più in generale dell'economia globale;

b) **centralità del fattore umano**, che mantiene un ruolo cruciale nelle fasi di sviluppo e convalida dei modelli, mediante il coinvolgimento degli opportuni stakeholder coerentemente con le peculiarità dei modelli stessi, nonché nelle fasi di controllo a valle, per il tramite di processi finali opportunamente documentati;

c) **trasparenza, accuratezza ed esplicabilità dei modelli**, tramite l'implementazione di: un processo di sviluppo e convalida strutturato, governato da strumenti IT secondo le best practice di riferimento e adeguatamente documentato; interfacce IT *user friendly* e supporto formativo per il loro utilizzo, in particolare al fine di garantire che l'output del modello sia coerente con quanto definito in fase di progettazione;

d) **sicurezza informatica, robustezza e *safety***, grazie ai sistemi ICT in uso che assicurano il governo integrato e documentato del ciclo di vita dei modelli (ivi compresa la tracciabilità dei dataset utilizzati), dei relativi processi e delle decisioni assunte in sede di sviluppo e di convalida degli stessi, ed infine l'analisi dei risultati ottenuti.

Il Gruppo FinecoBank adotta un approccio basato sul rischio coerentemente con il Regolamento del Parlamento Europeo, assicurando il rispetto dei seguenti requisiti aggiuntivi per i sistemi di AI ad alto rischio tenendo sempre in considerazione i principi sopra riportati:

a) conservazione, qualità, accuratezza e replicabilità dei dati sottostanti i predetti modelli, del controllo delle versioni degli algoritmi e della documentazione a supporto.
b) resilienza sia per quanto riguarda errori, guasti o incongruenze che possono verificarsi all'interno del sistema o nell'ambiente in cui esso opera, in particolare a causa della loro interazione con persone fisiche o altri sistemi, sia ai tentativi di terzi non autorizzati di modificare l'uso o le prestazioni del sistema di AI ad alto rischio.

Il rispetto dei principi sopra evidenziati opera anche come elemento di garanzia a presidio dei principi di sostenibilità del Gruppo, nonché della mitigazione circa l'esposizione ai rischi di natura reputazionale per il Gruppo FinecoBank.
Il Gruppo FinecoBank si impegna a porre particolare attenzione agli aspetti sotto riportati coerentemente con le linee guida / regolamentazioni emesse in materia di AI:

- **Trasparenza e accountability,** attraverso una chiara ed adeguata informativa laddove sia prevista l'interazione con sistemi di AI, specificando anche la tipologia di dati raccolti e le loro modalità di utilizzo da parte dei sistemi.
  I sistemi di AI utilizzati dal Gruppo mantengono una forte attenzione agli esseri umani in quanto tali, ponendosi come strumenti di supporto al fine di consentire loro di mantenere sempre un ruolo centrale in tutti i processi decisionali; inoltre, i sistemi utilizzati sono caratterizzati da una forte componente di innovazione, finalizzata a migliorare sempre la *customer experience* per renderla quanto più possibile fluida ed intuitiva su tutti i canali. La

soddisfazione dei clienti in termini di *user experience* nell'utilizzo dei servizi offerti dalla Banca e affidabilità e sicurezza degli stessi rappresentano un elemento chiave del Gruppo;

- **Etica ed equità:** Il Gruppo FinecoBank si impegna a sviluppare sistemi di AI in modo etico ed equo al fine di accrescere la fiducia da parte degli utilizzatori degli stessi. È importante assicurare che i risultati ottenuti con tali sistemi guidino tutti gli individui nelle proprie decisioni in modo equo e senza discriminazione e che i dati utilizzati dai sistemi siano, ove possibile, adeguatamente anonimizzati o pseudo-anonimizzati. Inoltre, il Gruppo FinecoBank, per tramite delle strutture tempo per tempo identificate in fase di implementazione della presente GP, garantisce un'adeguata sorveglianza umana deputata al controllo sul funzionamento ed utilizzo dei sistemi di AI; infatti, tutti gli esperti coinvolti nello sviluppo e diffusione dei sistemi di AI sono soggetti al Codice di Condotta del Gruppo, che include disposizioni esplicite per l'equità di trattamento, contro ogni discriminazione e pregiudizio.
  Il Gruppo FinecoBank si impegna a mitigare qualsiasi divario digitale che possa verificarsi a causa di un differente accesso alle tecnologie basate sull'Intelligenza Artificiale, anche attraverso l'attenta sensibilizzazione verso i propri partner e fornitori.
- **Privacy e sicurezza:** Particolare attenzione a queste tematiche è sempre garantita fin dalla fase di progettazione dei sistemi di AI, quali fattori abilitanti alla corretta definizione delle soluzioni offerte, anche cogliendo eventuali opportunità derivanti dall'evoluzione del contesto normativo nel quale il Gruppo opera, allo scopo di assicurare piena sicurezza per gli utilizzatori dei sistemi di AI, pur garantendo la semplicità di utilizzo.
  Il contesto è caratterizzato da una crescente complessità digitale e la sicurezza delle informazioni è diventata di cruciale importanza per il settore bancario.
  I passi compiuti per migliorare la gestione della sicurezza informatica contribuiscono a mitigare l'esposizione del Gruppo ai rischi operativi e reputazionali nonché alle vulnerabilità e alle minacce in continua evoluzione. Vengono infatti adottate le misure di sicurezza necessarie a mitigare i rischi inerenti ai servizi offerti, applicando le best practice di mercato in materia di sicurezza e garantendo l'unitarietà nel Gruppo della visione gestionale del rischio ICT, nonché l'uniformità di applicazione delle norme in materia di sistemi informativi.
- **Diritti umani, diversità ed inclusività:** Il Gruppo FinecoBank riconosce l'importanza del rispetto dei diritti umani, sostenendo l'imprescindibilità di questo elemento per una corretta condotta aziendale. Il Gruppo, inoltre, impronta le proprie attività alla garanzia e alla promozione del rispetto di tutti i diritti umani definendo un approccio inclusivo e assicurando il rispetto delle normative e degli standard nazionali ed internazionali in materia. L'impegno del Gruppo è finalizzato alla promozione della diversità e inclusività al fine di consentire la creazione di una cultura aziendale che garantisca un ambiente di lavoro scevro da ogni forma di discriminazione nel rispetto della dignità umana. L'impegno sui diritti umani riguarda anche la catena di fornitura, con l'obiettivo di minimizzare i rischi di violazione dei diritti stessi; a tale scopo, il Gruppo ha reso più efficiente la valutazione dei fornitori in relazione agli impatti sociali e ambientali, valutando le caratteristiche della catena di fornitura anche in termini di rispetto e protezione dei diritti umani. Tale impegno è dimostrato anche dall'adozione delle migliori pratiche nell'ambito dell'AI.
- **Massimizzare i benefici dell'IA mantenendo la centralità del fattore umano**: coerentemente con la sua natura digitale, il Gruppo FinecoBank è determinato a investire sempre di più sul business digitale pur mantenendo il fattore umano al centro del proprio business come fattore critico di successo.
  In un contesto caratterizzato da una crescente complessità digitale, è rischioso affidarsi alla sola tecnologia e, pertanto, il fattore umano continua a rappresentare uno degli anelli di protezione più importanti per il Gruppo Fineco ed è essenziale continuare a garantire che ci sia consapevolezza e presidio delle possibili minacce, sia da parte dei clienti che dei dipendenti e del management, per saperle riconoscere ed essere in grado di reagire in modo adeguato.

Fineco riconosce inoltre che l'utilizzo dell'AI può svolgere un ruolo di primaria importanza nel percorso di perseguimento degli obiettivi di innovazione e sostenibilità ambientale e sociale del Gruppo, lungo tutta la sua catena del valore.

L’utilizzo di modelli di AI può infatti contribuire alla riduzione dell’impatto ambientale delle attività svolte, ad esempio promuovere un uso più sostenibile delle risorse, attraverso il monitoraggio e l’analisi di dati e i processi gestiti attraverso AI. I dati prodotti e gestiti dalle AI possono inoltre essere utilizzati per comprendere i processi legati al cambiamento climatico e per sviluppare di conseguenza nuovi modelli in grado di migliorare la gestione dei rischi ambientali.

Sotto il profilo sociale, il rispetto dei principi di equità, diversità e non discriminazione nella strutturazione e nell’applicazione dell’AI favoriscono la riduzione delle disuguaglianze, contribuendo a promuovere e a migliorare accessibilità e inclusione.

3. CLASSIFICAZIONE E GESTIONE DEI MODELLI

Con riferimento alla classificazione e trattamento dei modelli di *Artificial Intelligence* secondo un approccio basato sul rischio, il Gruppo Fineco si impegna ad applicare il Regolamento dell'Unione Europea, Artificial Intelligence Act (AI Act), che stabilisce regole armonizzate sull'intelligenza artificiale e modifica alcuni atti legislativi pregressi emanati dall'Unione Europea.

Con riferimento alla definizione degli algoritmi di *Artificial Intelligence*, il Gruppo segue il Regolamento e – in linea con il parere formulato dalla Banca Centrale Europea – adotta un approccio "basato sul rischio" per l'impiego di tali algoritmi. Questo approccio prevede che, a un livello di rischio maggiore, corrispondano regole d'uso più rigorose.

In particolare, il Gruppo applica il modello di classificazione suddiviso in: i) rischio inaccettabile; ii) rischio alto; iii) rischio limitato; e iv) rischio minimo.

Il Gruppo intende rispettare questa classificazione e si impegna a adottare le seguenti pratiche, sulla base delle suddette classi di rischio:

Pratiche di AI per rischio inaccettabile

Non implementare pratiche di Intelligenza Artificiale che presentino un rischio inaccettabile per la sicurezza, i mezzi di sussistenza e i diritti delle persone. In particolare, sono proibiti:

- I sistemi di sfruttamento della vulnerabilità delle persone tramite tecniche subliminali, manipolative ed ingannevoli;
- I sistemi di categorizzazione biometrica delle persone fisiche per dedurne o desumerne etnia, opinioni politiche, appartenenza sindacale, convinzioni religiose ed orientamento sessuale;
- I sistemi di identificazione biometrica (riconoscimento facciale) in tempo reale in spazi accessibili al pubblico;
- I sistemi di riconoscimento delle emozioni utilizzati sul luogo di lavoro, eccetto che per motivi medici o di sicurezza;
- L'estrazione non mirata (*scraping*) di immagini facciali da internet o da telecamere a circuito chiuso per la creazione o espansione di banche dati;
- I sistemi che consentono di attribuire un "punteggio sociale" (*social scoring*), classificando o valutando le persone in base al loro comportamento sociale o alle loro caratteristiche personali.

Pratiche di AI per sistemi ad alto rischio

Implementare i sistemi ricadenti in questa categoria ottemperando a tutte le prescrizioni definite nell'AI Act, in particolare procedendo a dimostrare che ciascun sistema è conforme ai requisiti obbligatori per una IA affidabile (ad esempio qualità dei dati, documentazione, tracciabilità dei dati e dei modelli, sorveglianza umana, accuratezza, cybersecurity e robustezza).

I sistemi devono essere tecnicamente robusti per garantire che la tecnologia sia adatta allo scopo e che i risultati, in termini di accuratezza e di falsi positivi/negativi, non incidano in maniera sproporzionata (*bias*) su gruppi protetti (ad esempio per origine etnica, sesso, età, ecc.). I sistemi devono, inoltre, essere addestrati e testati con set di dati sufficientemente rappresentativi dei dati del Gruppo, per ridurre al minimo il rischio di integrazione di distorsioni inique che, se presenti, devono essere risolte mediante opportune correzioni ed attenuazioni. I dati utilizzati per l'addestramento ed il testing dell'algoritmo devono anche essere tracciabili e verificabili, garantendo la conservazione dell'opportuna documentazione nel rispetto della normativa tempo per tempo applicabile in materia di trattamento di dati personali, ivi incluso il Regolamento (EU) 2016/679.

Infine il Gruppo si impegna ad effettuare una valutazione d'impatto sui diritti fondamentali delle persone, che consista nella descrizione dei processi in cui il sistema di AI sarà utilizzato, del periodo temporale e delle frequenze in cui il sistema è destinato ad essere utilizzato, delle categorie di persone fisiche e di gruppi che potrebbero essere interessati dal suo uso, dei rischi specifici di danno che posso incidere sulla categorie di persone e gruppi che lo utilizzeranno, e nella descrizione delle misure di sorveglianza umane e delle misure da adottare in caso i rischi si concretizzino.

Per i sistemi ad alto rischio si fa riferimento all'elenco contenuto nell'AI Act (Allegato III), specificando qualora l'ambito Non sia Applicabile (**OOS-out of scope**) al Gruppo:

- Sistemi di identificazione/categorizzazione biometrica, protetti dall'Articolo 9(1) del Regolamento (EU) 2016/679, per cui sono esclusi sistemi AI utilizzati per l'autenticazione remota finalizzata all'accesso ai servizi del Gruppo da parte dei clienti, che non sono considerati ad alto rischio;
- Sistemi relativi alla valutazione dell'occupazione, mirati ad ottimizzare la gestione dei lavoratori e l'accesso al lavoro autonomo (ad esempio, per pubblicare annunci di lavoro mirati, analizzare e filtrare le candidature e valutare i candidati);
- Sistemi finalizzati alla valutazione dell'affidabilità creditizia delle persone fisiche, alla valutazione dei rischi finanziari, nonché alla determinazione dei prezzi in relazione ad assicurazioni sulla vita e assicurazioni sanitarie;
- Sistemi finalizzati alle attività di Anti-Money Laundering (AML), utilizzati con l'obiettivo di prevenire, identificare, investigare e perseguire attività illecite;
- (**OOS**) Sistemi utilizzati come componenti di sicurezza nella gestione e nel funzionamento delle infrastrutture digitali critiche, del traffico stradale e della fornitura di acqua, gas, riscaldamento ed elettricità;
- (**OOS**) Sistemi finalizzati a determinare l'accesso, l'ammissione o l'assegnazione agli istituti di istruzione e formazione professionale (ad esempio, per valutare i risultati dell'apprendimento e orientare il processo di apprendimento e il monitoraggio dei comportamenti disonesti);
- (**OOS**) Sistemi usati per determinare l'accesso a servizi e a prestazioni pubblici e privati essenziali (come, ad esempio, l'assistenza sanitaria);
- (**OOS**) Sistemi utilizzati nelle attività di contrasto, di gestione della migrazione, dell'asilo e del controllo delle frontiere, di amministrazione della giustizia, nonché nello svolgimento dei processi democratici e per la valutazione e classificazione delle chiamate di emergenza.

Un sistema di AI di cui all'Allegato III è sempre considerato ad alto rischio qualora esso effettui profilazione di persone fisiche.

Sistemi a rischio limitato

Implementare, come definito dall'AI Act, meccanismi di trasparenza per i sistemi di AI legati a questa categoria. In particolare, il Gruppo si impegna a introdurre meccanismi di comunicazione e di trasparenza volti a informare i clienti sull'impiego diretto di sistemi basati sull'intelligenza artificiale. Questo consentirà ai clienti di effettuare scelte consapevoli riguardo alla continuazione dell'utilizzo dei servizi AI a rischio limitato. FinecoBank si impegna a rendere chiaramente riconoscibile ai clienti l'interazione con un sistema AI, permettendo loro di decidere consapevolmente se proseguire o meno nel suo utilizzo. Il Gruppo si impegna ad assicurare che i contenuti generati tramite AI sotto forma di testo, immagini e video siano chiaramente identificabili.

Sistemi a rischio minimo

Rispettare quanto descritto dall'AI Act per questa categoria, fermo restando l'allineamento al Codice di Condotta del Gruppo. All'interno di questa casistica rientrano sistemi di AI utilizzati per la classificazione automatica di documenti, l'estrazione automatica di dati strutturati da fonti non

strutturate, l'automazione di processo, la revisione automatica di documenti (per tono, stile e linguaggio, *brand* del Gruppo), la scoperta automatica di anomalie, soluzioni *smart* per la gestione documentale (indicizzazione, ricerca, processamento del testo e del parlato, *entity liking*, traduzione documentale), ossia tutti quei sistemi di AI che non influenzano le decisioni o gli interessi delle persone o che offrono un supporto secondario ad attività svolte in prima persona dalle persone.

In aggiunta all'approccio basato sul rischio, il Gruppo segue le linee guida etiche del 2019 per l'IA affidabile, sviluppate dall'indipendente *High Level Expert Group on Artificial Intelligence* (AI HLEG) nominato dalla Commissione europea. In tali linee guida, l'AI HLEG ha sviluppato sette principi etici non vincolanti per l'AI, che sono intesi a garantire che l'AI sia affidabile ed eticamente corretta. I sette principi sono: intervento e sorveglianza umani; robustezza tecnica e sicurezza; privacy e governance dei dati; trasparenza; diversità, non discriminazione e equità; benessere sociale e ambientale e responsabilità.

Relativamente ai sistemi di G*eneral Purpose AI* (GPAI), come *Foundational Models* (Modelli Fondativi) *e Large Language Models (LLM)*, ossia per modelli con più di 10^25 FLOPS, il Gruppo si impegna a rispettare quanto prescritto nell'AI Act, ossia che tutti questi modelli rientreranno nella categorizzazione di rischio relativa alla integrazione in sistemi di AI quando messi sul mercato. In caso di utilizzo per fine di ricerca o esperimenti interni non verranno considerati ricadenti nella casistica dei sistemi ad alto rischio. Inoltre, il Gruppo si impegna, in caso di pubblicazione sul mercato di sistemi GPAI, ad applicare le raccomandazioni relative ai *rischi sistemici*.

La propensione al rischio nell'utilizzo di modelli AI ad alto rischio è stabilita all'interno del Risk Appetite Framework (nell'ambito del Risk Appetite Statement). L'utilizzo di modelli AI ad alto rischio da parte del Gruppo è limitato, e, nei limiti del possibile, confinato ad un utilizzo interno e soggetto ai presidi di controllo di primo e secondo livello coerentemente con il sistema dei controlli interni e di gestione dei rischi della Banca. In tal senso, l'eventuale adozione di un modello AI ad alto rischio è equiparata ad una Operazione di Maggior Rilievo (c.d. OMR, la cui valutazione ed approvazione segue il processo definito nella Global Policy Operazioni di Maggior Rilievo, a cui si rimanda per pronto riferimento).

Anche allo scopo di monitorare l'adozione dei c.d. sistemi di intelligenza artificiale ad alto rischio nei confronti delle persone fisiche, il Gruppo si impegna a creare e gestire un catalogo interno relativo a tutti i modelli AI utilizzati (sviluppati internamente o da fornitori esterni), che elenchi caratteristiche e finalità, illustri il presidio dei principi adottati dal Gruppo, nonché contenga una valutazione di rischio da parte delle funzioni di primo e secondo livello, incluse le valutazioni di conformità per i modelli ad alto rischio.

4. Ruoli e Responsabilità

4.1 Responsabilità della Capogruppo

Per governare in modo efficace l'IA e garantire che venga impiegata in modo sicuro e responsabile, nel rispetto delle normative di riferimento è fondamentale definire un modello organizzativo, che preveda la definizione e assegnazione di ruoli e responsabilità all'interno del Gruppo e delle sue Società.

Il Gruppo si impegna, per il tramite delle funzioni coinvolte (a titolo esemplificativo e non esaustivo: Global Business, Sostenibilità, DPO, risk management, compliance, legale, BPR, ICT, Sicurezza, risorse umane, ecc.), ad effettuare una valutazione per ambito di competenza delle iniziative progettuali che prevedano l'uso di sistemi di AI per il tramite dei processi interni di demand e project management. A titolo esemplificativo:

- DPO, in coerenza con le attuali attribuzioni, sorveglia che l'applicazione dell'AI non pregiudichi la conformità alla normativa tempo per tempo applicabile che disciplina il trattamento dei dati personali
- Legal, in linea con le proprie attribuzioni e competenze, per l'ambito AI, garantisce conformità alle norme applicabili, quali a titolo esemplificativo e non esaustivo, in merito alla proprietà intellettuale, accordi di licenza e alla definizione dei contratti verso fornitori, clientela e più in generale verso parti terze;
- Sostenibilità, in coerenza con le proprie attribuzioni, per l'ambito AI, garantisce il rispetto dei principi di etica e di equità, nonché il rispetto delle risorse ambientali.

Inoltre, Fineco, con riferimento alla Capogruppo integra i principi in materia di Artificial Intelligence nel suo sistema di governance, assegnando, o confermando ove già in essere, responsabilità agli organi di governo e alle funzioni aziendali, come delineato di seguito:

- il Consiglio di Amministrazione, in qualità di organo con funzione di supervisione strategica, approva le politiche strategiche in materia di Artificial Intelligence, avvalendosi preliminarmente del supporto dei comitati endoconsiliari, quali, principalmente, Comitato Rischi e Parti Correlate e Comitato Corporate Governance e Sostenibilità Ambientale e Sociale, ciascuno per quanto di competenza;
- l'Amministratore Delegato e Direttore Generale, in qualità di Organo con Funzione di Gestione, ha il compito, anche in ambito AI, in coerenza con le attuali attribuzioni, di assicurare la completezza, l'adeguatezza, la funzionalità e l'affidabilità del sistema informativo, in aggiunta: mette a punto i piani di azione contenenti le misure da adottare per conseguire gli obiettivi della strategia ICT, ne monitora e misura l'efficacia, ne cura il riesame periodico, dandone informativa al Consiglio di Amministrazione; approva, almeno con cadenza annuale, il piano operativo delle iniziative informatiche, verificandone la coerenza con le strategie aziendali e le esigenze informative e di automazione delle aree di business; assicura la definizione dei ruoli e le connesse responsabilità per la funzione ICT e per la gestione del rischio ICT e di sicurezza; approva le procedure e i processi di gestione delle operazioni ICT concernenti le risorse e i servizi non esternalizzati, garantendo l'efficacia e l'efficienza dell'impianto nonché la complessiva completezza e coerenza;
- ICT & Security Office (CIO): in coerenza con le attuali attribuzioni, per l'ambito AI, assicura la predisposizione, l'adozione e la gestione della normativa interna in materia di ICT e Security,

supporta l'Amministratore Delegato e Direttore Generale nella definizione (e aggiornamento in base alle necessità) dei Piani di azione per la successiva approvazione in Consiglio di Amministrazione, contenenti le misure da adottare per attuare la strategia ICT; garantisce la predisposizione del piano operativo relativo alle iniziative informatiche, verificandone la coerenza con le strategie aziendali; sottopone lo stesso piano all'approvazione dell'Amministratore Delegato e Direttore Generale; predispone e cura l'adozione delle policy e linee guida in tema di Artificial Intelligence;

- Outsourcing Management: è responsabile di coordinare i flussi informativi interni volti ad assicurare agli Organi Aziendali e alle Funzioni Aziendali di Controllo della Banca la corretta e completa valutazione dell'esposizione della Banca ai rischi derivanti dai servizi ICT forniti da terze parti e dagli accordi di esternalizzazione;
- Compliance, in linea con le proprie attribuzioni, per l'ambito AI, verifica che le procedure e i processi interni siano adeguati a prevenire il rischio di non conformità in materia di AI, inclusi gli aspetti relativi al trattamento dei dati personali, alla sicurezza informatica, anche attraverso la misurazione del rischio stesso;
- Risk Management, in coerenza con le proprie attribuzioni, concorre per l'ambito AI, all'analisi dei rischi ICT e di sicurezza ed è responsabile del monitoraggio e del controllo di tali rischi, assicurando che gli stessi siano individuati, misurati, valutati, gestiti e mitigati, monitorati nonché riportati e mantenuti entro i limiti della propensione al rischio della banca;

È consentito, ove lo si ritenga, che possano costituirsi specifici gruppi di lavoro, tempo per tempo identificati a seconda delle necessità o delle fattispecie.

4.2 Responsabilità delle Società controllate

L'Entità controllata destinataria, con riferimento al governo dei modelli AI (*Artificial Intelligence*) utilizzati dal Gruppo e alla loro implementazione nel rispetto delle regole di Sicurezza delle Informazioni, ha la responsabilità di:

- adottare ed implementare le regole e le linee guida definite all'interno del presente documento, con riferimento alla governance dei modelli ed alla sicurezza delle informazioni, in coerenza e conformità con le specificità locali e le leggi e regolamentazioni vigenti in materia;
- collaborare alla condivisione e conoscenza dei possibili rischi che impattano il Gruppo;
- fornire reportistica periodica in merito al corretto rispetto dei principi elencati nella presente Global Policy.