Extract of the policy on the development and responsible use of artificial intelligence

Unipol

EXTRACT OF THE POLICY ON THE DEVELOPMENT AND RESPONSIBLE USE OF ARTIFICIAL INTELLIGENCE

Milan, August 7th, 2025

Table of Contents

Document objectives

The Policy aims to define the guidelines of the Unipol Group (the "**Group**") on the development and responsible use of artificial intelligence ("**AI**") systems.

In this regard, the Policy establishes, in relation to companies of the Group falling within its scope of application:

- the organisational model for the control of AI risk.
- the guidelines governing the development and responsible use of AI systems, including the fundamental principles adopted by the Group with regard to AI.
- the processes governing the development and responsible use of AI Systems, the obligations applicable to High-Risk AI Systems and the related reporting obligations.
- the provisions regarding the monitoring of AI systems, the selection and management of Third Parties and training on the subject of AI.
- the roles and responsibilities in the use and development of AI systems and the related reportingflows.

Unless otherwise specified, the bodies/areas/functions referred to the Policy shall be understood as referring to Unipol Assicurazioni S.p.A. ("**Unipol**") and, where applicable, to the equivalent bodies/areas/functions of the other In-Scope Companies, including where outsourced.

Regulatory references

The Policy was drafted in compliance with regulations in force and the sector supervisory policies reported below.

European legislation:

- Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 establishing harmonised rules on artificial intelligence (the "AI Act").
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons in relation to the processing of Personal Data and the free movement of such data (the "GDPR").
- Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector (the "DORA") and its related delegated regulations.
- Report on Artificial intelligence governance principles: towards ethical and trustworthy artificial intelligence in the European insurance sector, issued by the Consultative Expert Group on Digital Ethics in Insurance of EIOPA (the "EIOPA Guidelines").

Domestic regulations:

- Italian Legislative Decree No. 58 of 24 February 1998: TUF - Consolidated Law on Finance.
- Italian Legislative Decree No. 209 of 7 September 2005 - the Private Insurance Code, as subsequently amended (the "Private Insurance Code").
- Italian Legislative Decree No. 196 of 30 June 2003, the "Personal Data Protection Code" (the "Privacy Code"), as subsequently amended and supplemented.
- Supervisory Provisions for Payment Institutions and Electronic Money Institutions issued by the Bank of Italy on 17 May 2016, as subsequently amended and supplemented.
- IVASS Regulation No. 38 of 3 July 2018 containing provisions on the corporate governance system, as subsequently amended and supplemented.
- Bank of Italy Provision of 5 December 2019 implementing Articles 4-undecies and 6, paragraph 1 (b) and (c-bis) of the Consolidated Law on Finance ("TUF"), as subsequently amended and supplemented.

The Policy is also consistent with and forms an integral part of the self-regulatory framework in force within the Group.

Scope of application

The Policy applies to the Parent Company and to companies controlled by it within the Group that have their registered offices in Italy that develop or use AI Systems (collectively the "In-Scope Companies").

Regarding the fundamental principles identified by Unipol, the Policy also applies to companies of the Group that do not have their registered offices in Italy, which shall in any case adopt their own policy consistent with the Policy.

Definitions and terminology

Training data	The data used to train an AI system by adapting the metrics it can learn.
Validation data	The data used to evaluate the trained AI System and to fine-tune, inter alia, parameters that cannot be learned and the learning process, inter alia, in order to prevent insufficient (*underfitting*) or excessive (*overfitting*) adaptation to the Training Data.

Test data	The data used to provide an independent assessment of the AI System in order to confirm its expected performance before its placing on the market or putting into service.
Personal Data	Any information concerning an identified or identifiable natural person; a natural person is considered identifiable if they can be identified, directly or indirectly, with particular reference to an identifier such as a name, identification number, location data, online identifier or one or more characteristic elements of their physical, physiological, genetic, psychological, financial, cultural or social identity.
Beneficiary	Natural or legal person who is affected by the AI System, even without directly interacting with it. It may affect the user.
DPIA or *Data Protection Impact Assessment*	Impact assessment on the protection of Personal Data.
IA Room	*Team* coordinated by the AI Governance Function and composed of the Parent Company's corporate functions and the corresponding functions within the In-Scope Companies involved, entrusted with supporting the Proposing Function in the assessment of AI Risk: *Compliance, Information*, *Innovation and Risk* areas, *the Corporate Social Responsibility* function*, the Organisation* function (or, where appointed, the BC Manager), and *the Ethics Officer.* The AI Governance Function may seek support from other corporate functions based on the assessment needs identified.
Serious Incident	An incident or malfunction of an AI System that, directly or indirectly, results in one of the following consequences: (i) the death of a person or serious harm to a person's health, (ii) a breach of obligations under Union law intended to protect fundamental rights, (iii)

	serious damage to property or the environment.
IT Incident	Single event or series of unplanned related Events with negative impact on the Integrity, Authenticity, Availability and / or Confidentiality of ICT systems and Services and related data.
AI model	The physical, mathematical or otherwise logical representation that underlies an AI System. It includes, inter alia, statistical models and various types of *input-output* functions (such as decision trees and neural networks).
Prohibited AI practices	The issue on the market, commissioning or use of AI systems that pose an unacceptable risk to the rights and freedoms of Users under the AI Act.
Profiling	Any form of automated Processing of Personal Data consisting of the use of such Personal Data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's work performance, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
Register of AI Systems, or Register	Group IT platform that allows the registration of the AI systems developed/in use by the Group, as well as the related technical documentation, supervised by the AI Control Unit and maintained on an ongoing basis by the Proposing Functions.
Accessibility requirements	Technical requirements that the AI System must meet in order to be usable by all natural persons, including those with disabilities.
Requirements for the management of AI risk	Requirements for the management of AI Risk of AI Systems, broken down according to a risk-based approach.

AI risk	This refers to the set of risks derived from the development and use of an AI System (e.g. risk of non-compliance with regulations, operational risk, reputational risk, strategic risk, etc.).
AI system	An automated system designed to operate with varying levels of autonomy and that may exhibit adaptability after deployment, and that, for explicit or implicit objectives, infers from the input it receives how to generate outputs such as predictions, content, recommendations or decisions that can influence physical or virtual environments. Several AI Systems can be supported by the same AI Model.
High Risk AI system	AI system that poses a significant risk to the rights and freedoms of Users according to the criteria defined in the AI Act.
Medium-High Risk AI system	AI system which, although not classifiable as a High Risk AI system, may pose significant risks for the Recipients and/or for the In-Scope Companies.
Low- or Medium-Risk AI System	AI system that does not pose significant risks for the Recipients or for the In-Scope Companies.
Generative AI system	AI system that generates audio, image, video or textual content in response to a user prompt or request.
User	Natural person who materially uses or interacts directly with the AI System. Recipients are also considered Users, when the AI Systems are also designed to interact directly with them.

Organisational model for monitoring risks derived from the use of AI

In order to ensure effective governance of AI Risk, both during the development and the use of an AI System, the *governance* process within the Parent Company and the In-Scope Companies must be clearly and consistently defined.

The Group has defined roles and responsibilities, both at the Parent Company level and at the subsidiary level, that ensure the governance, implementation, and oversight of the model for managing risks arising from the use of AI (the "**Model**").

Area	**Objective**
Guidance and governance	Guarantee the definition and promote the dissemination and correct implementation of the Model, as well as the strategies for the ethical and responsible development and use of AI.
Execution	Guarantee the implementation of the defined Model, in compliance with the applicable internal and external provisions.
Control	Identify, assess, manage and monitor the risks derived from the use of AI.

Guidelines on the development and responsible use of AI systems

AI regulations aim to promote the ethical, responsible and secure development of AI Systems, while ensuring the protection of fundamental rights and the safety of Users and Recipients.

The Unipol Group's approach to the development and use of Artificial Intelligence is based on ethics principles, which ensure that technologies are used for the benefit of people and the community.

The following fundamental principles guide all phases of the life cycle of the AI systems developed and used within the Group:

Transparency, explainability, security and reliability

The Group recognises that transparency is essential for building trust in the use of Artificial Intelligence. The Group is committed to ensuring that AI Systems are developed and used in a manner that makes their objectives, general functioning and main decision-making logic understandable to Users and Recipients. Where applicable, customers will be informed in a clear and accessible manner about the use of AI in the services and products offered.

From a transparency perspective, the explainability of outputs produced by AI Systems is of particular importance. Therefore, among the solutions adopted by the Group, methods and tools are provided which, in particular where transparency for the protection of Recipients is considered necessary, enable the reconstruction of how a specific *output* was generated from the *input* provided.

Additionally, the Group considers safety and reliability to be essential aspects in the development and adoption of AI systems, for which the AI Models are designed to ensure technical robustness and minimise the risk of unexpected errors or unexpected behaviour. To this end, the Group adopts validation, *testing* and ongoing monitoring processes to ensure compliance with high standards of quality, cybersecurity and resilience.

Furthermore, with regard to Artificial Intelligence systems that involve direct interaction with individuals, such as *chatbots*, virtual assistants, and content generators, the Group is committed to ensuring that the User is clearly and unequivocally informed that they are interacting with an AI System. These systems are designed to provide accurate, relevant, verifiable and complete answers. In-Scope Companies shall, in any case, always ensure that the User has the possibility to interact with a human operator.

Equity and algorithmic non-discrimination

Regarding the use of Artificial Intelligence, the Group is committed to preventing the creation or amplification of unjustified discrimination by adopting measures aimed at ensuring the impartiality and accuracy of the data used and monitoring the fairness of the *outputs* generated by the models.

Particular attention is paid to the detection and mitigation of any *bias*[3], i.e. undesirable trends in the results produced by the technology. These deviations can in fact produce negative effects both with regard to the objectives that are intended to be pursued with the use of the technology, and, potentially, undermine the principles of inclusiveness, equality and non-discrimination.

Human supervision and oversight

The Group recognises the importance of human supervision and oversight in the design, implementation and control of AI systems. Automated decision-making processes provide for the

possibility of monitoring, understanding, and, where necessary, intervening in the functioning of AI Systems and, where possible, in the *output* produced through human oversight. Human oversight contributes to ensuring that AI operates in compliance with ethics principles, fundamental rights and current regulations, while maintaining ultimate control and responsibility with the designated human operators.

Privacy and data protection

The adoption of AI Systems shall be implemented in accordance with the principles set out in the Policy on the protection and enhancement of Personal Data, in force periodically, ensuring respect for the rights, fundamental freedoms and dignity of Data Subjects, the minimisation of the data processed, transparency towards Data Subjects, and the security of data throughout the entire lifecycle of AI Systems.

In line with this framework, the Group reaffirms its commitment to:

- ensure that any processing of Personal Data is performed in compliance with the rights, fundamental freedoms and dignity of the data subjects.
- implement adequate technical and organisational measures to prevent unauthorised access, loss, alteration or unlawful processing of Personal Data.
- ensure clear, comprehensive, and easily accessible communication to Data Subjects regarding the methods and purposes of data processing.
- promote the responsible use of Personal Data, fostering awareness and understanding of the impacts that AI technologies may have on individuals.
- use data in a manner that creates value for customers, stakeholders and the community, without ever compromising the rights and legitimate expectations of Data Subjects.
- ensure, where applicable, that the use of special categories of data (e.g. biometric, healthcare, sensitive data) takes place only where an appropriate legal basis exists and under conditions of strict necessity, in accordance with Art. 9 (2) (g) of the GDPR and Art. 10 (5) of the AI Act.
- ensure that the datasets used for the training, validation and testing of High-Risk AI Systems are selected and processed in such a way as to be relevant, sufficiently representative and to the extent possible free of errors and complete with regard to the intended purpose, in accordance with Art. 10 (3) of the AI Act.

Environmental sustainability and responsible innovation

The Group, in view of its awareness of the environmental impact associated with the development and use of AI, promotes an approach based on responsible practices that take environmental sustainability into account, encouraging the adoption of technological solutions with reduced energy

consumption and lower environmental impact, in line with its Sustainability Policy and the Group Climate Change Strategy.

In this context, the Group encourages the voluntary adoption of additional requirements that contribute to the sustainability of AI, including the eco-friendly design of models, the optimisation of computational consumption, and the measurement and mitigation of the environmental footprint of the solutions developed or adopted. Particular attention is given to the integration of environmental criteria also within innovation and technological experimentation processes, involving external *stakeholders* such as research, academic, or civic organisations, in order to promote a comprehensive approach to responsible innovation.

Collaboration and stakeholder participation

The Group values dialogue and *stakeholder* engagement as an essential element for the development of Artificial Intelligence that is sustainable, responsible and in line with the expectations of civil society.

In the development, use and monitoring of AI systems, the Group is committed to:

- considering, where applicable, the needs and expectations of customers, business partners, employees and the community;
- guaranteeing respect for the rights of customers, business partners, employees and other stakeholders;
- promote - where appropriate - the active participation of internal and external stakeholders in the definition of guidelines, policies and operating practices on AI;
- maintain an open dialogue with regulatory bodies, industry associations, the scientific community and civil society organisations in order to share good practices in relation to AI governance models.

This approach aims to guide the adoption of AI by the Group so that it is integrated with the economic, social and environmental context in which it operates.

The Group recognises that the successful adoption of Artificial Intelligence in a responsible manner depends decisively on the awareness and competence of its people.

To this end, the Group promotes ongoing communication, engagement and training initiatives aimed at raising employees' awareness, with the objective of:

- promoting a corporate culture oriented towards the ethical and responsible use of AI through the use of the Intranet Futura and all internal digital channels (Communities of Practice, UniDuello, brochures, engagement meetings, etc.);
- providing basic knowledge on the principles of transparency, fairness, security and data protection applicable to AI systems;

- ensuring that employees are aware of the potential risks associated with the use of AI and the behaviour to be adopted to prevent or report them;
- supporting the development of technical and management skills functional to the design, development, implementation and monitoring of AI systems.

The training programmes are calibrated according to the different roles and levels of responsibility, guaranteeing adequate preparation of all those directly or indirectly involved in the processes related to AI.

Fundamental Rights Impact Assessment (FRIA)

Where a High-Risk AI System intended to be developed and used is designed to assess the creditworthiness of natural persons, establish their credit score, or for risk assessment and pricing in relation to life and health insurance, an assessment of the impact that the use of such System may have on the fundamental rights of Users (*Fundamental Rights Impact Assessment* or "**FRIA**") shall be performed in accordance with the procedures set out in the Group DCA.

Once completed, the FRIA shall be submitted for signature by the Chief Executive Officer or, where not present, the General Manager of the Company and transmitted to the Authorities in accordance with the procedures indicated by them.

If, during the use of the AI System, it is considered that any of the elements analysed in the FRIA has changed or is no longer updated, the Group shall adopt the necessary measures to update the information.

Monitoring of AI Systems

AI Systems in use at the In-Scope Companies are subject, in accordance with a *risk-based* approach, to a monitoring system throughout their lifecycle, aimed at:

verifying that the data is processed in compliance with applicable regulations, particularly regarding the protection of Personal Data, copyright and any sector-specific regulations.

- ensuring the continuous updating of the technical documentation supporting the AI System;
- identifying potential errors or malfunctions of the AI System;
- guaranteeing the quality and improvement of the performance of the AI System;
- with particular reference to generative AI systems, preventing the generation and/or dissemination of harmful, violent, misleading or illegal content;
- verifying which Users use the AI Systems, ensuring consistency with information recorded in the Register.

To this end, the Group adopts tools that enable the automated monitoring of AI Systems based on KPIs defined during the design, development, validation, or evaluation of AI Systems.

In-Scope Companies acting as *Developers* of High-Risk AI Systems shall establish a plan for their post-deployment monitoring, which forms an integral part of the technical documentation and enables the ongoing verification of their compliance with applicable regulatory requirements, including on the basis of information provided by *Deployers*, throughout their lifecycle.

AI communication and training

Each employee, in relation to their role and area of responsibility, shall develop and use only the AI Systems for which they have been authorised, in compliance with the regulations periodically in force and ensuring effective management of AI Risk.

To this regard, communication plans and dedicated training programmes are established to ensure a sufficient level of AI literacy and adequate awareness of the risks associated with the use of AI Systems not subject to the governance process, including the potential compromise or disclosure of confidential corporate data, including non-personal data.

The training courses established, in order to ensure adequate training of *Deployers*, include:

- basic elements of AI and its ability to influence business processes (AI Awareness), as well as the mechanisms and rationale for such influence, including knowledge of the regulatory and operational aspects associated with AI (AI Literacy);
- training plans specifically dedicated to company functions dedicated to the design and development of AI systems.

Additionally, specific *induction* sessions are reserved for the Board of Directors.

The training courses take into account:

- the role covered by the different company functions, as well as the individual AI systems to which they have been enabled;
- where applicable, any human supervision tasks assigned;
- the technical knowledge, experience, education and training of the different company functions;
- the context in which the AI Systems are to be used and, where applicable, the Recipients.

In the event of a breach of the procedures and limits governing the use of AI Systems, disciplinary measures may be applied in accordance with the applicable sector National Collective Labour Agreements (CCNL).