

4IG INFORMATION TECHNOLOGY LTD.

ARTIFICIAL INTELLI- GENCE CODE OF ETHICS

Identifier	Version	Effective	Related regulation	Access restriction
COM14_4iGIT	1.0	18/08/2025	COM7_4iGIT_Code of Ethics and Business Conduct COM6_4iGIT_Code of Ethics for Business Partners	Public

RELEASE

Regulatory function	Name	Operation	Position	Date of approval / Signature
Process owner	Melinda Kurucz	Group Compliance	Compliance specialist	
Signatory for compliance	Dr. Éva Szántó	Group Legal and Regulatory Directorate	Head of Legal Affairs	
Signatory for compliance	Richárd László Somodari	Information security	Head of the IT Security Department	
Signatory for compliance	Dalma Andriska	Group Quality Management and Regulatory Directorate	Group Head of Quality Management and Internal Regulatory	
Signatory for compliance	Melinda Kurucz	Group Compliance	Compliance specialist	
Signatory for compliance	Szilvia Rommevaux	Group Corporate Governance and Operational Development	Group Head of Corporate Governance and Operational Development	
Signatory for compliance	Dr. Judit Lerch	IT Business Portfolio Management Directorate	Head of IT Business Portfolio Management	
Approver	Gábor Radó	Office of the Chief Executive Officer	Chief Executive Officer	

DOCUMENT HISTORY

Version	Date of entry into force	Short description of modification
1.0	18/08/2025	Issue of new rules

DEFINITIONS

Definition	Explanation
Company	4iG Information Technology Ltd
Artificial intelligence, Artificial intelligence system, AI system, AI	A machine-based system designed to operate at 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, content, recommendations or decisions that may influence physical or virtual environments.
Business partner	All business organisations and natural persons having a contractual relationship other than an employment relationship with 4iG Information Technology Ltd., including but not limited to suppliers, subcontractors, distributors, agents, representatives, customers, clients and joint venture partners.
Trade secret	A fact, information, other data or a compilation thereof, related to economic activity, that is secret, in whole or in the configuration and combination of its elements, in that it is not generally known or readily accessible to persons who normally deal with such information in the course of the economic activity concerned, and which consequently has commercial value, where the person lawfully in control of the secret has taken steps that may reasonably be expected in the given circumstances to keep it secret.
Inside information	Inside Information (MAR) means information of a precise nature which has not been made public and which relates directly or indirectly to one or more issuers or one or more financial instruments and the making public of which would be likely to have a significant effect on the prices of those financial instruments or related derivative financial instruments. Once disclosed, Inside Information necessarily loses its insider nature. Further detailed rules on Inside Information are set out in Clause 2 of these Rules.
4iG Group/Group	4iG Nyrt. and all member companies under the direct or indirect sole or majority control of 4iG Nyrt.

APPLICABLE LAWS

Name

Universal Declaration of Human Rights of the United Nations (United Nations General Assembly Resolution 217 A, adopted on 10 December 1948)

Act No. 8 of 1976 on the promulgation of the International Covenant on Civil and Political Rights, adopted by the General Assembly of the United Nations at its twenty-first session on 16 December 1966

Act XXXI of 1993 on the promulgation of the Convention for the Protection of Human Rights and Fundamental Freedoms, signed in Rome on 4 November 1950, and the eight Protocols thereto

Charter of Fundamental Rights of the European Union

Treaty on the Functioning of the European Union

Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No. 300/2008, (EU) No. 167/2013, (EU) No. 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144, and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act, AI Act)

Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

CONTENT

1. Scope and Responsibilities	5
1.1 Purpose of the Rules	5
1.2 Responsibility	5
1.3 Scope	6
1.3.1 Personal Scope	6
1.3.2 Term	6
1.3.3 Objective scope	6
2. Framework for Trustworthy Artificial Intelligence.....	6
2.1 Lawful Artificial Intelligence.....	7
2.2 Ethical artificial intelligence	8
2.2.1 Respect for Fundamental Rights	8
2.2.2 Respect for Human Autonomy and Human Oversight	9
2.2.3 Prevention of Harm.....	9
2.2.4 Fairness and Proportionality	9
2.2.5 Transparency and Explainability	10
2.2.6 Protection of Privacy and Personal Data	10
2.2.7 Protection of Trade Secrets, Intellectual Property and Confidential Information	10
2.2.8 Fair Trade and Competition	11
2.2.9 Fair Working Conditions	11
2.2.10 Accountability	11
2.3 Robust Artificial Intelligence	12

1. SCOPE AND RESPONSIBILITIES

1.1 PURPOSE OF THE RULES

The purpose of the Artificial Intelligence Code of Ethics (hereinafter the “**AI Code of Ethics**” or the “**Code**”) is to establish, in line with the vision of 4iG Information Technology Ltd. (hereinafter “we” or “us”) and the principles and values set out in our Code of Business Conduct and Ethics, the fundamental framework that enables the incorporation and application of fundamental values and expectations in the development, deployment and use of artificial intelligence (hereinafter “**artificial intelligence**”, “**artificial intelligence system**”, “**AI system**” or “**AI**”) applications.

To this end, the AI Code of Ethics sets out the standards of conduct to be followed by our executive officers and employees, thereby contributing to the long-term and consistent preservation of our strong ethical foundations in the context of AI applications and systems as well.

As a key player in the Hungarian information technology and telecommunications services market, we consider it important to shape professional thinking and public perceptions regarding AI systems through our active participation in professional dialogue on AI-based technological solutions, and to contribute to shaping society’s perception of AI through our ethical practices and the consistent communication of our professional position.

We remain firmly committed to providing our customers with state-of-the-art, high-quality and secure services by applying the most effective technological solutions available in line with the prevailing state of technology; this includes making AI systems available to our customers. In pursuing our efforts in the interests of our customers, we must pay particular attention to following practices for the trustworthy use of artificial intelligence and to supporting the business activities of our business partners exclusively through ethical AI systems.

This AI Code of Ethics shall be interpreted in accordance with the principles, values and framework set out in the Code of Business Conduct and Ethics of 4iG Information Technology Ltd.

The purpose of this AI Code of Ethics is also to set out the principles and basic standards necessary to create an ethical culture and operations that comply with the law and internal policies, and to define expected business conduct with regard to AI systems. This helps to identify situations that may arise in the course of work and may constitute a breach of ethical standards during the development, implementation, and use of AI applications and systems.

Group Compliance is responsible for interpreting this AI Code of Ethics and for providing guidance in relation to it.

1.2 RESPONSIBILITY

All executive officers and employees of 4iG Information Technology Ltd. are responsible for complying with the provisions of this Code. Where a business partner (in particular, a supplier) is involved in the

design, development or use of an AI system, the employee or organisational unit that has an interest in the development, testing or use of the AI system shall be responsible for ensuring that the principles set out in this Code are upheld in relation to such business partner.

1.3 SCOPE

1.3.1 Personal Scope

The rules set out in the Code apply to all employees of 4iG Information Technology Ltd., including executive officers.

Our business operations and success are based on ambitious objectives, outstanding performance and fair business conduct under all circumstances, in compliance with the law, internal policies and professional and ethical rules. Business partners also play a significant role in achieving these objectives, as, for the purposes of this Code, they may play an important role in the development, testing and use of AI systems.

We therefore expect our business partners to also commit to the principles and commitments set out in this AI Code of Ethics, to familiarise themselves with and adhere to the ethical and compliance principles that we uphold, and to apply these principles to AI systems within their own operations and throughout their respective value chains.

Our business partners are expected to take measures proportionate to the size, complexity and risk exposure of their organisations to ensure ethical AI systems. We expect our partners to inform 4iG Information Technology Ltd. Compliance without delay of any information they become aware of in relation to a breach of the AI Code of Ethics and the results of any internal procedure (self-audit) conducted on the basis of such suspicions, through the Ethics and Compliance Line established by 4iG Information Technology Ltd. for this purpose.

1.3.2 Term

This Code shall enter into force on the day following its promulgation. These Rules are valid for an indefinite period of time.

1.3.3 Objective scope

This Code sets out the ethical framework governing the use and development of Artificial Intelligence by 4iG Information Technology Ltd.

2. FRAMEWORK FOR TRUSTWORTHY ARTIFICIAL INTELLIGENCE

AI is a rapidly evolving technology that can deliver wide-ranging economic and societal benefits; however, we recognise that the elements and techniques that enable the economic benefits of artificial intelligence may also give rise to new risks or adverse consequences for individuals or society. In view of this, efforts should be made to maximise the opportunities offered by AI systems while managing and mitigating the risks associated with their use.

In the course of our business activities, we may use AI systems across a wide range of areas, including, among others, our operations, management and the provision of services. We may also sell AI systems

developed in-house or by third parties. Given the anticipated role of AI systems in our business processes, as well as the potential impacts and risks associated with the use of AI, we are committed to developing and using AI systems in a responsible, safe, accountable, transparent, fair and ethical manner, and to using only **trustworthy** AI systems.

For the purposes of this AI Code of Ethics, AI shall be considered trustworthy where the following three conditions are cumulatively satisfied throughout the entire lifecycle of the system, namely that artificial intelligence is:

- a) **lawful**,
- b) **ethical**, and
- c) **robust** from a technical, social and environmental perspective.

Accordingly, we are committed to developing, operating and selling only trustworthy artificial intelligence applications that comply with the principles of lawfulness, ethics and robustness.

2.1 LAWFUL ARTIFICIAL INTELLIGENCE

The requirement of lawfulness in relation to artificial intelligence means that we comply with the requirements set out in all relevant legislation in force at any given time concerning the development, sale and use of artificial intelligence.

When ensuring compliance with the requirement of lawfulness, consideration must be given to the legal frameworks that apply to the development and use of artificial intelligence, whether as horizontal requirements applicable to all activities or as specific requirements applicable to certain industries or activities. These requirements may arise from international conventions, EU law or Hungarian legislation, as well as from the legislation of other states that are relevant to our operations.

This may include horizontal legislation that generally governs the organisation's operational framework and is applicable to all of our activities; examples include:

- human rights conventions that are closely related to the requirements applicable to ethical artificial intelligence, such as the Charter of Fundamental Rights of the European Union or the European Convention on Human Rights;
- statutory requirements relating to the processing of personal data, such as the General Data Protection Regulation ("GDPR");
- general statutory requirements applicable to artificial intelligence, such as the Artificial Intelligence Act ("AI Act");
- further statutory requirements relating to discrimination, such as Act CXXV of 2003 on Equal Treatment and the Promotion of Equal Opportunities;
- statutory requirements relating to fair market conduct and the prohibition of restrictions on competition, such as Articles 101 and 102 of the Treaty on the Functioning of the European Union and Act LVII of 1996 on the Prohibition of Unfair Market Practices and Restrictions of Competition;
- Directive (EU) 2022/2464 on corporate sustainability reporting ("CSRD");
- Regulation (EU) 2023/2772 on sustainability reporting standards ("ESRS").

The requirement to take into account legislation relating to specific industry requirements or activities will always depend on the scope of the use of artificial intelligence. This means that, by examining the purpose for which artificial intelligence is being used, it must be determined whether specific industry legislation is applicable in relation to the use of artificial intelligence.

Examples include:

- specific statutory requirements applicable to the electronic communications sector, which establish the operational requirements of the industry, such as Act C of 2003 on Electronic Communications;
- legislation prescribing consumer protection requirements and providing for the enforcement of consumer rights, such as Act CLV of 1997 on Consumer Protection and Act XLVII of 2008 on the Prohibition of Unfair Commercial Practices against Consumers.

2.2 ETHICAL ARTIFICIAL INTELLIGENCE

Our responsibility, however, does not stop at the limits of lawful operation. Social responsibility is, on the one hand, an integral part of our operations; this includes the expectation that we should lead by example even where the challenges arising from the rapidly changing environment associated with technological development cannot be fully addressed by the applicable legal rules. For another thing, a cornerstone of our operations is to conduct our business, including procurement, development, sales, service delivery, and communications, in a manner that complies at all times with the highest ethical standards. This is particularly important in situations characterised by an imbalance of power, where one party is significantly less able to assert and enforce its interests than the other party. Such situations may arise, for example, in the relationship between an employer and an employee, or between businesses and consumers. In such cases, particular emphasis may need to be placed on upholding ethical expectations in relation to the use of artificial intelligence.

When applying ethical principles and standards relating to artificial intelligence, we must consider both the impact that the development, sale and use of AI systems may have on us and the direct or indirect effects of these activities on our business partners, customers, competitors and other relevant third parties.

This AI Code of Ethics identifies ten such ethical considerations that contribute to the development and use of ethical artificial intelligence.

2.2.1 Respect for Fundamental Rights

Fundamental rights are universal rights that safeguard and protect the freedom and autonomy of every individual. The requirement to respect fundamental rights is closely linked to the requirement for lawful artificial intelligence, as fundamental rights are defined and safeguarded by international conventions and legislation.

With regard to the substance of these fundamental rights, we consider the relevant legal instruments, in particular the United Nations Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, the Charter of Fundamental Rights of the European Union and the Fundamental Law of Hungary, to be authoritative.

We are committed to respecting the fundamental rights of individuals and to upholding these rights in the development and use of artificial intelligence. In particular, we consider the following fundamental rights to be of particular relevance to the use of artificial intelligence:

- the right to life,
- the right to human dignity,
- the right to physical and mental integrity,
- the right to respect for private and family life,
- the right to the protection of personal data,
- the right to liberty and security,

- freedom of thought, conscience and religion,
- freedom of expression and information,
- the right to property,
- the prohibition of discrimination,
- equality between women and men,
- the rights of the child.

2.2.2 Respect for Human Autonomy and Human Oversight

In order to safeguard fundamental rights, individuals interacting with AI systems must be enabled to fully and effectively retain their personal autonomy, make free and informed decisions concerning themselves, and act freely. Appropriate mechanisms must therefore be established to ensure, on the one hand, effective human oversight of artificial intelligence throughout its entire lifecycle and, on the other hand, that individuals are not subject to decisions made by artificial intelligence that may produce legal effects or similarly significant effects on them, and that such decisions remain subject to human decision-making.

In this regard, we develop and use AI systems that, in accordance with the principle of respect for human autonomy, support human autonomy and decision-making, while ensuring that the workflows of AI systems can be supervised and controlled.

2.2.3 Prevention of Harm

The rights to life, human dignity and personal integrity can be safeguarded where AI systems and the environments in which they operate are robust and secure. AI systems must not cause harm, exacerbate existing harm or otherwise adversely affect people. To this end, we exclude the possibility of malicious use intended to cause harm and, where there is a risk that AI systems may cause or exacerbate adverse impacts, for example as a result of information asymmetries, we are committed to implementing appropriate measures to prevent or mitigate such harm.

2.2.4 Fairness and Proportionality

Irrespective of age, gender, abilities or other characteristics, we make decisions regarding the provision or use of a particular service solely on the basis of business considerations that are consistent with the principles set out in this AI Code of Ethics and the Code of Business Conduct and Ethics. At the same time, the operation of AI systems may result in inferences drawn from data relating to natural persons that lead to unfair outcomes, potentially resulting in unintended direct or indirect harm to, or discrimination against, certain individuals or groups of people.

For this reason, we develop and use only applications for which the accuracy of the data, the use of appropriate models and appropriate oversight of the AI system in this regard can be ensured.

The requirement of proportionality is closely linked to the principle of fairness. This means that the use of AI systems must not go beyond what is necessary to achieve a particular purpose. The requirement of proportionality must always be interpreted in the context of the purpose intended to be achieved through the use of artificial intelligence. The principle of proportionality must be upheld to ensure that the solutions developed through the design, testing and use of AI systems respect fundamental rights and that, from the perspective of fundamental rights, the least adverse measures are implemented.

2.2.5 Transparency and Explainability

The safeguarding of fundamental rights, respect for human autonomy, prevention of harm, and the principles of fairness and proportionality can be ensured where processes are transparent, AI systems are identifiable, and their capabilities and purposes are publicly available and understandable, and where decisions made by artificial intelligence can be explained. To this end, 4iG Information Technology Ltd. informs individuals when they are interacting with artificial intelligence.

In the use of artificial intelligence, it must therefore be ensured that individuals are able to make independent and informed decisions when interacting with AI and are able to understand and assess the potential impact of artificial intelligence on them. It must also be ensured that individuals, in particular users, are aware that they are using or interacting with artificial intelligence in the course of their interactions with us.

Where a particular outcome or decision cannot be explained, or cannot be fully explained, in the context of the use of a particular artificial intelligence application, other forms of control must be put in place; these may include ensuring the traceability and auditability of the system's capabilities, as well as providing transparent information about them.

We seek to explain decisions made by AI to the individuals concerned wherever possible and to provide them with appropriate information about the impact of artificial intelligence on them, thereby ensuring that they have the opportunity to autonomously request human review of decisions made by artificial intelligence.

2.2.6 Protection of Privacy and Personal Data

We are committed to protecting privacy and personal data; accordingly, we develop, sell and use only AI applications for which the protection of privacy, personal data and the rights of data subjects in relation to the processing of personal data can be ensured and demonstrated at every stage of the AI system lifecycle.

In the development and use of AI systems, we process personal data only in compliance with the GDPR and other applicable legal requirements. In the development and use of AI systems, we collect and use personal data only in a fair and lawful manner.

When using artificial intelligence, we ensure that the quality of the data used is appropriately considered in order to prevent biases that could lead to violations of fundamental rights. Such potential issues must be identified before the processing of personal data begins and appropriately addressed through suitable measures in order to prevent violations of fundamental rights.

2.2.7 Protection of Trade Secrets, Intellectual Property and Confidential Information

Both during the development and use of AI systems, trade secrets or other information relating to intellectual property, as well as information that is confidential for other reasons (such as inside information), may be uploaded to AI systems. In addition, data or information that constitutes inside information, a trade secret or intellectual property may also be generated during the operation of an AI system or as a result thereof. The protection of such information is of particular importance to us.

When using AI systems, employees are required to treat and safeguard as trade secrets any information, facts, data, opinions or knowledge that comes to their attention concerning us, our customers or our business partners, and may not use such information for their own benefit or for the benefit of any third

party, or disclose it to any third party. The Employee shall remain bound by this obligation of confidentiality even after termination of the employment.

Consequently, particular care must also be taken with regard to information used in AI systems where the use of artificial intelligence involves our own or our business partners' trade secrets, confidential information or intellectual property. The use of a business partner's or customer's trade secrets, confidential information or intellectual property in an AI system is permitted only with the consent of the relevant customer or business partner. It is strictly prohibited to use such information without obtaining the necessary authorisation. Similarly, any intellectual property protected by a third party must be respected.

Where employees create, in the course of their employment, a work using artificial intelligence that is capable of being protected by intellectual property rights or is protected by law from the moment of its creation, they may not use such work for their own purposes.

Furthermore, care must be taken to ensure that information uploaded to an AI system does not become accessible to unauthorised persons. As a consequence, data constituting a trade secret or intellectual property, as well as confidential information, may only be uploaded to an AI system within the framework specifically established for this purpose.

2.2.8 Fair Trade and Competition

In the development and use of AI systems, any form of unfair market conduct that would unlawfully undermine the image or reputation of competitors must be avoided. Furthermore, practices that distort, restrict or eliminate competition through the use of artificial intelligence are not permitted. Accordingly, artificial intelligence must not be developed or used in a manner that constitutes an abuse of a dominant position or that, whether directly or indirectly, results in price determination or price fixing between competitors, market allocation, allocation of customers or suppliers, or any other restriction, distortion or elimination of competition.

2.2.9 Fair Working Conditions

Artificial intelligence can make a significant contribution to the work of employees; however, given the nature of the employment relationship, particular attention must be paid to ensuring that the use of artificial intelligence does not undermine employees' rights or result in the unlawful monitoring of employees.

Furthermore, the use of artificial intelligence must not result in the infringement of the fundamental rights of employees or persons seeking to enter into an employment relationship; in particular, artificial intelligence must not be used to discriminate between employees.

Particular caution must be exercised in relation to the use of artificial intelligence by employers, and the interests of employees must be taken into account in order to prevent risks and potential harm arising from the power asymmetry between the parties.

Organisations must use AI applications that affect employees or consumers in a transparent manner, ensuring fairness, inclusivity, freedom from bias and respect for human rights, while aligning the requirements of the AI Act with the social standards set out in the ESRS.

2.2.10 Accountability

In accordance with the principle of accountability, we establish and apply a framework that ensures that the operation of AI systems and their impact on the internal and external environment can be traced and

audited, that responsibilities relating to the operation of AI systems can be clearly defined, and that compliance with statutory and ethical requirements can be ensured, demonstrated and documented throughout the entire lifecycle of the AI system.

2.3 ROBUST ARTIFICIAL INTELLIGENCE

Technical robustness is a key element in achieving trustworthy artificial intelligence and is closely linked to the principle of *prevention of harm*. AI systems must be developed and used in a sustainable and environmentally responsible manner. As AI systems may inadvertently cause harm, they must operate safely, reliably and robustly, and appropriate measures must be taken to prevent undesirable adverse impacts. The use of artificial intelligence may give rise not only to internal but also to external risks. With regard to external risks, appropriate measures must be taken to ensure that AI systems are resilient to external attacks at the data, model, software and hardware levels.

AI systems must be developed using a risk-prevention approach, in such a way that they operate reliably and as intended, while minimising unintended and unexpected harm and preventing unacceptable harm. Monitoring processes must be put in place to ensure safety and reliability.