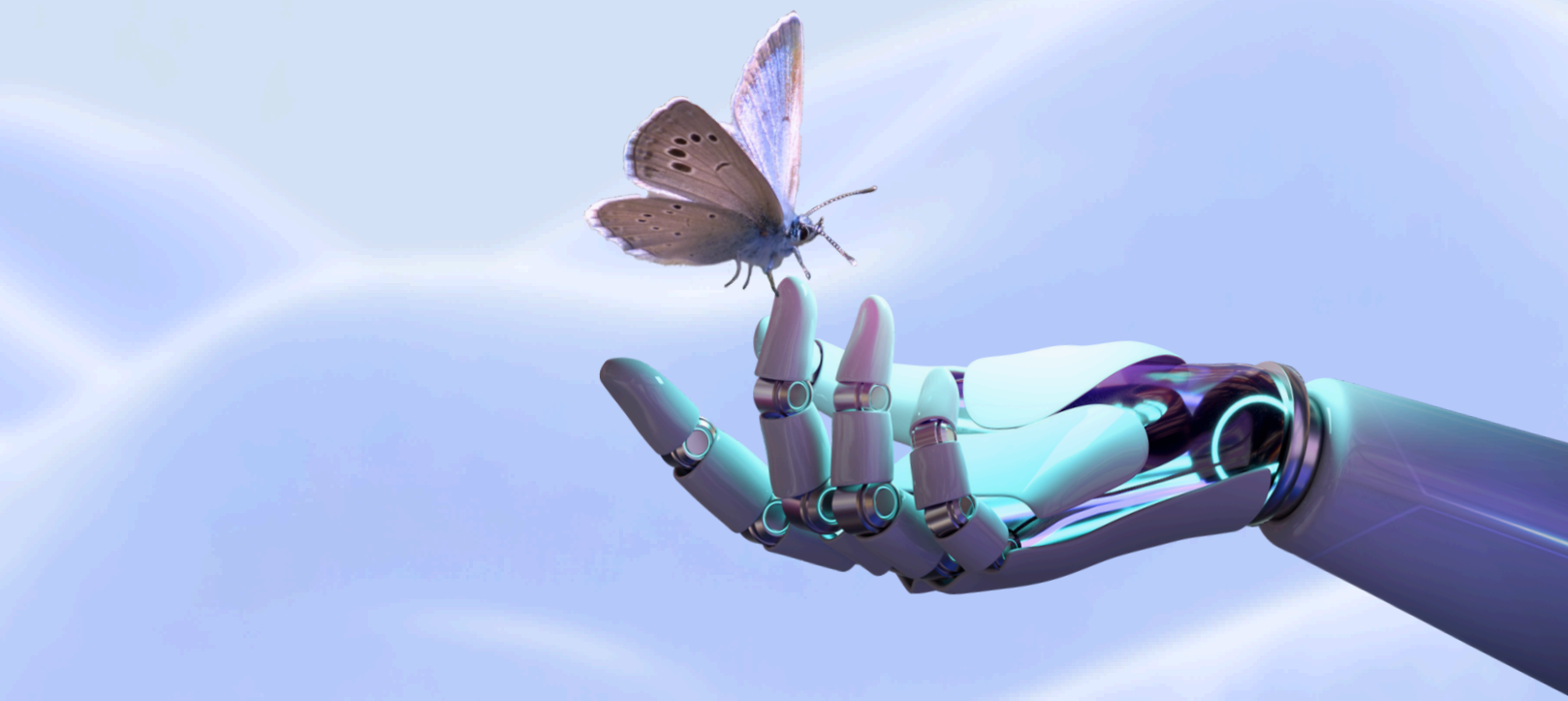
VOLUNTARY CODE OF CONDUCT

ON THE ETHICAL AND RESPONSIBLE USE OF **ARTIFICIAL INTELLIGENCE**



16.12.2024

EXPLANATORY NOTE

Artificial Intelligence (AI) systems are rapidly evolving, permeating all aspects of our lives—from customer support chatbots to complex data analysis, decision-making systems, and even recruitment processes. The widespread adoption of AI systems makes the implementation of the ethical principles outlined in this Voluntary Code of Conduct on the Ethical and Responsible Use of Artificial Intelligence (hereinafter referred to as the "Code") critically important for companies. By adhering to these ethical principles, companies developing AI can prevent the spread of biases, discrimination, and unintended harm. Ethical adherence strengthens trust and accountability, fostering societal benefits such as improved decision-making processes, enhanced privacy protection, and sustainable and inclusive progress in key sectors, including healthcare, education, and public administration.

INTENDED AUDIENCE

This Code is designed for:

- Companies that develop or utilize AI systems across a wide range of applications, such as generative systems, enterprise knowledge management tools, customer service solutions, and other similar technologies;
- Developers, researchers, legal professionals, and managers working with these systems;
- Civil society organizations involved in the regulation and implementation of AI technologies.

PURPOSE

The purpose of this Code is to ensure that AI business representatives uphold human rights as outlined below, fostering a culture of self-regulation in the field of AI within Ukraine. This is aimed at promoting the ethical and responsible use of artificial intelligence.

The Code outlines a series of measures that companies signing the Code (hereinafter referred to as "Signatory Companies") are expected to undertake to:

- Identify, Avoid, or Mitigate Risks. Ensure that potential risks related to human rights compliance associated with AI systems are identified, avoided, or mitigated while promoting the ethical use of AI. The Code aims to guarantee that AI systems do not violate human rights.

- Foster a Culture of Self-Regulation. Promote the development of a culture of self-regulation in the field of AI in Ukraine. This Code seeks to create an environment where AI developers assume responsibility for the ethical development and use of their systems.

- Ensure Consistency and Transparency. Provide a unified approach to collaboration between various organizations and companies working in the AI sector. Such consistency is crucial for transparency, regulatory compliance, and building trust among stakeholders.

- Raise Staff Awareness. Encourage the enhancement of awareness among the staff of Signatory Companies about AI systems, offering tools for informed decision-making when working with AI systems to uphold ethical principles and respect human rights.

VOLUNTARY CODE OF CONDUCT ON THE ETHICAL AND RESPONSIBLE USE OF ARTIFICIAL INTELLIGENCE

8 Principles for the Ethical and Responsible Use, Development, and Governance of Artificial Intelligence Systems

SCOPE AND APPLICABILITY

Recognizing that AI carries risks to human rights, freedoms, and society as a whole that require careful management and aspiring to foster responsible and ethical development and use of AI, the Signatory Companies voluntarily commit to applying AI in a manner that aligns with the highest ethical standards. They also pledge to advance the development and adoption of responsible AI practices. Within the limits permissible for the Signatory Companies (taking into account internal policies, NDA provisions, agreements on trade secrets, and other contracts and obligations), they agree to implement the principles outlined in this Code.

This Code does not address issues related to the development or use of AI systems in the national security and defence sectors.

The degree and level of implementation of each principle listed below must align with the specific characteristics of the respective system and the level of potential AI risks, as defined by the OECD AI Risk Classification Framework.

TERMS AND DEFINITIONS

Input Data refers to data provided to or directly received by the AI system, based on which the system produces output data.

Lifecycle includes planning and designing the system; collecting and processing data in compliance with current and international legislation; building the AI system(s) and/or adapting existing AI system(s) for specific purposes; testing, evaluating, verifying, and validating; deploying and releasing to the market; operating and monitoring; as well as decommissioning, discontinuing, or destroying the AI system.

Training Data refers to data used to train the AI system by adjusting its trainable parameters.

Risk refers to the combination of the likelihood of adverse outcomes and the severity of those outcomes.

User refers to an individual who interacts with a service, application, platform, or other tool that operates fully or partially based on an AI system, regardless of the purpose or manner of such interaction.

Signatory Company Personnel refers to the collective employees and contractors engaged by the operator in various stages of working with AI systems. This includes activities such as development, testing, deployment, implementation, maintenance, as well as dissemination and monitoring of AI systems.

Artificial Intelligence System (AI System) refers to a machine-based system designed to operate with varying levels of autonomy and capable of demonstrating adaptability after deployment, which, for explicit or implicit purposes, infers from input data it receives how to generate output data such as predictions, content, recommendations, or decisions that may affect the physical or virtual environment.

Applicable Legislation refers to the set of legal acts adopted by the government authorities of Ukraine, as well as international treaties, conventions, and other international legal documents ratified by Ukraine and having legal force on its territory.

The terms personal data owner, personal data controller, personal data, personal data processing, personal data processing that poses particular risks to the rights and freedoms of personal data subjects, and personal data subject are used as defined in the Law of Ukraine dated 01.06.2010 No. 2297-VI "On Personal Data Protection."

PRINCIPLE 1: RISK-BASED APPROACH

Signatory Companies must acknowledge their responsibility for the AI systems they develop or manage and, when necessary, take appropriate technical and organizational measures, as determined at their discretion, to manage risks and ensure the safe and responsible use of such systems throughout their lifecycle.

Compliance with this principle may include, but is not limited to, the following:

- Identification and assessment of potential risks and impacts of AI on human rights at various stages of the AI system lifecycle.
- Development and implementation of organizational and technical measures to manage risks, proportionate to the nature of the activity and the risks of the AI system, taking into account its entire lifecycle.
- Developing and implementing policies, procedures, and staff training aimed at ensuring the ethical and responsible use of AI.
- Updating AI systems to address security vulnerabilities and improve their performance.
- Developing and implementing crisis protocols to ensure timely and appropriate responses to identified risks, including their mitigation or elimination of negative consequences.
- Sharing information and best practices in risk management with other Signatory Companies while maintaining confidentiality as necessary.
- Applying various testing methods and measures to evaluate, address, and reduce security risks and discriminatory biases in AI systems prior to market release.
- Providing personnel responsible for working with AI systems with updated guidelines on the proper use of the AI system, including information on measures taken to address and minimize risks

PRINCIPLE 2: SAFETY AND ROBUSTNESS

Signatory Companies must take appropriate measures to ensure the safety of users and the reliability of AI systems throughout their lifecycle.

Compliance with this principle may include, but is not limited to, the following:

- Establishing procedures for reporting security incidents and documenting recorded incidents in the operation of AI systems, along with subsequent remediation of security gaps.

- Applying diverse testing methods across various tasks and contexts prior to deployment to evaluate performance and ensure the reliability of AI systems. Signatory Companies may independently determine the most appropriate testing methods for their AI systems, taking into account potential risks.

- Implementing cybersecurity measures deemed appropriate by the Signatory Company to protect AI systems from attacks, including data encryption and access control.

- Conducting training and internal testing on digital security and cybersecurity for staff and involved individuals, tailored to the Signatory Company's specific needs and the potential risks associated with their AI systems.

PRINCIPLE 3: PRIVACY AND DATA PROTECTION

Signatory Companies must design, implement, and process personal data within the lifecycle of AI systems in compliance with applicable data protection legislation.

Compliance with this principle may include, but is not limited to, the following:

- Notifying data subjects about the sources of data collection, the transfer of personal data to third countries, the purpose of data processing, and the location of the Signatory Company as the data controller or processor.
- Informing data subjects about the mechanism of automatic data processing, including automated decision-making that has legal consequences for the individual, the logic and criteria of such decisions, and the possibility of human review of those decisions.
- Establishing and documenting the legal basis for processing personal data in AI systems, including recording exceptional cases where the processing of personal data poses particular risks to the rights and freedoms of data subjects.
- Implementing appropriate organizational and technical measures to protect data and prevent breaches, such as accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access to personal data. Signatory Companies determine the necessary measures proportionate to the risks, such as information security policies, data encryption, access controls, and regular backups.
- Engaging only processors that provide sufficient guarantees of implementing the required technical and organizational measures to ensure compliance with applicable laws and protect the rights of data subjects.
- Adhering to the principle of data minimization, collecting and processing only the personal data necessary to achieve the specific purpose of processing within AI systems.

PRINCIPLE 3: PRIVACY AND DATA PROTECTION

- Adherence to the principle of data retention limitation, ensuring that personal data processing identifies data subjects only as long as necessary to achieve the purpose of processing within AI systems or as defined by applicable law.
- Ensuring the accuracy and reliability of data, reviewing databases when necessary to maintain the information in a truthful and up-to-date form, considering the purpose of such data processing.
- Providing users with access to their personal data and the ability to correct or delete it in accordance with applicable legal requirements.
- Establishing procedures for conducting privacy impact assessments (DPIA/PIA) to evaluate and mitigate potential risks to privacy.
- Implementing principles of privacy by design and privacy-enhancing technologies to embed privacy protections throughout the AI system lifecycle.
- Using pseudonymization techniques to minimize the risk of identifying data subjects, where necessary, at the discretion of the Signatory Company and proportional to the associated risks.
- Establishing procedures for data deletion or anonymization after the expiration of the data processing and storage period, in compliance with applicable legal requirements.
- Appointing a designated person or department responsible for organizing personal data protection activities, where required by law, to ensure compliance in data processing practices.
- Implementing mechanisms for rapid detection, response, and resolution of incidents related to data breaches or violations of personal data protection within the Signatory Company.
- Conducting periodic training and internal testing for the Signatory Company's personnel on responsible handling of personal data within AI systems.

PRINCIPLE 4: EQUITY AND FAIRNESS

Signatory Companies must design AI systems in a way that avoids violations of human rights, discrimination, and biases at all stages of the AI system lifecycle, as well as ensure the representativeness of the data used as training data.

Compliance with this principle may include, but is not limited to, the following:

- Establishing a dedicated unit or appointing a responsible person to oversee the AI system, including conducting regular assessments of the system's impact on human rights and ensuring adherence to the principles outlined in the Code.
- Using representative datasets for training AI systems. These datasets should reflect the diversity of the population (including gender, age, social status, place of residence, etc.) to avoid biases and discriminatory outcomes in the system's operation.
- Refraining from the use of widely prohibited practices for AI systems, such as social scoring, manipulating human behaviour, or real-time facial recognition, unless explicitly permitted by applicable law.
- Managing training datasets for AI systems, including auditing datasets to identify and mitigate biases and discriminatory elements where possible, as well as ensuring their secure storage.

PRINCIPLE 5: TRANSPARENCY

Signatory Companies must ensure transparency in the functioning of AI systems and decision-making processes, provide clear information about AI systems' capabilities and limitations, and disclose the sources of data used for their training.

Compliance with this principle may include, but is not limited to, the following:

- Providing sufficient and user-friendly information about the capabilities and limitations of the AI system, including a general description of the algorithms used and the types of training data based on the AI system's risk and limitations. This information should enable consumers to make informed decisions.

- Developing and utilizing labelling methods where appropriate. For example, clear labelling or notifications to inform users that they are interacting with an AI system rather than a human, or messages indicating the system's limitations to warn users that the results may contain errors or may not be applicable in certain cases.

- Disclosing generalized descriptions of the types of training data used for system development without revealing confidential information, as well as measures taken to identify, mitigate, and minimize risks and details about testing conducted. Where possible, providing public access to datasets used to train the AI system.

- Properly and clearly inform users that they are interacting with an AI system.

PRINCIPLE 6: HUMAN OVERSIGHT AND MONITORING

Signatory Companies must provide the ability for AI system decisions to be reviewed and corrected by a human and grant users the right to challenge such decisions in cases where they have legal or other significant consequences for the user, or where they have a substantial impact on democracy, the rule of law, human rights, public order, public safety, or public health.

Compliance with this principle may include, but is not limited to, the following:

- Defining clear roles and responsibilities for structural units or individuals overseeing the AI system.
- Implementing monitoring procedures to track the performance of AI systems and identify potential issues, such as monitoring accuracy, impartiality, and fairness in system outputs.
- Establishing an accountability framework within the Signatory Company, including clear reporting mechanisms that allow employees to raise concerns, report unethical use of AI systems to responsible managers, and seek guidance from those managers.
- Incorporating provisions for periodic review and evaluation of AI systems into internal policies of the Signatory Companies to identify, address, and mitigate shortcomings and risks that may affect compliance with the principles of ethical and responsible AI use. The frequency and methods of review and evaluation should be determined by the Signatory Companies based on the risks and purpose of the AI system.
- Including commitments to ethical development and responsible use of AI systems in the job descriptions of the Signatory Company's personnel, aligned with the internal policies of the Signatory Company.
- Creating mechanisms or portals to receive feedback, complaints, and inquiries from users of AI systems and stakeholders. These mechanisms should enable communication with the individual overseeing the AI system and facilitate the provision of feedback.

PRINCIPLE 7: AWARENESS BUILDING AND LEADERSHIP

Signatory Companies should support initiatives aimed at developing and implementing innovative solutions, new standards, and methodologies, as well as undertake measures to raise user awareness in the field of ethical and responsible AI at their discretion and in accordance with their capabilities.

Compliance with this principle may include, but is not limited to, the following:

- Contributing to the development and implementation of industry standards to ensure the ethical and responsible use of AI.
- Investing in research and development for safe, reliable, and fair AI, including supporting academic research, establishing in-house research laboratories, and collaborating with other organizations, including civil society.
- Participating in the creation and implementation of educational programs for the public on the safe and ethical use of AI and sharing best practices.
- Collaborating with stakeholders, universities, and research centers to support studies focused on developing standards for the ethical and responsible use of AI.
- Working with relevant organizations to develop intellectual property (IP) legislation that meets the current needs and specificities of AI use.
- Jointly with other Signatories of the Code, promoting the development of sectoral implementing guidelines for the ethical and responsible use of AI.

PRINCIPLE 8: INTELLECTUAL PROPERTY

Signatory Companies commit to complying with applicable legislation in the field of intellectual property (IP) protection in the development and use of AI, including avoiding copyright infringement on software, training data used for AI system development, determining ownership of content generated by or with the use of AI systems, and ensuring the fair distribution of benefits derived from AI use.

Compliance with this principle may include, but is not limited to, the following:

- Timely adaptation of AI systems to comply with the requirements of national legislation and Ukraine's international obligations in the field of intellectual property (IP).

- Facilitating access to tools and procedures for stakeholders with legitimate interests, including rights holders, to exercise and protect their IP rights. For example, Conducting consultations regarding potential IP infringement and exploring possible solutions; and implementing notification and response systems to address potential IP rights violations.

COMMITMENTS DURING THE INITIAL IMPLEMENTATION PHASE OF THE CODE

Within six months from the date of signing the Code, Signatory Companies will make every effort to prepare for the implementation process of the Code's principles and reporting to ensure full compliance with its provisions. Compliance with the Code will be considered achieved if, during the reporting period, at least one example of the principles outlined in the Code is implemented, and its implementation is described in the report. The reporting period will begin six months after the signing of the Code. Simultaneously, Signatory Companies commit to actively supporting the establishment of a self-regulatory organization within six months of signing the Code. This organization will provide support, monitoring, and collaborative development of practices for compliance with the Code.

FINAL PROVISIONS

By signing this Voluntary Code of Conduct on the Ethical and Responsible Use of Artificial Intelligence (AI), the Signatory Companies voluntarily commit, within the limits permissible for them, to:

- Adhering to the principles and provisions outlined in this Code.
- Implementing and maintaining systems and processes to ensure compliance with these principles and provisions.
- Reviewing and updating their AI policies and practices to align with this Code and applicable legislation.
- Publishing annual reports among Signatory Companies at least once a year on their activities related to compliance with this Code.
- Publishing publicly accessible annual materials about their activities in implementing the provisions of this Code (e.g., AI-related blogs or similar content).
- Actively supporting the establishment of a self-regulatory organization to provide support, monitoring, and collaborative development of practices for compliance with this Code.

The reports should, among other things, include:

- A description of the measures and tools implemented by the Signatory Company aimed at fulfilling the principles and provisions of this Code.
- Information about any issues or challenges the Signatory Company encountered in connection with compliance with this Code.
- Plans of the Signatory Company for future activities aimed at fulfilling the provisions of this Code.

IMPORTANT:

This Code does not limit the requirements of national legislation and international law. It may be updated from time to time in accordance with technological and legislative advancements.

SIGNATORIES OF THE CODE

Grammarly
Mariana Romanyshyn, Area Tech Lead for Computational Linguistics

MacPaw
Volodymyr Kubytskyi, Head of AI

LetsData
Andriy Kusyy, CEO & Co-founder

DroneUA
Serhiy Malenkyi, Director

WINSTARS.AI
Dmitriy Sofyna, CEO R&D Center

Gametree.me
Bogdana Sydorenko, CEO

YouScan.io
Oleksii Orap, Founder & Chief Growth Officer

EVE.calls
Oleksii Skrypka, CEO & Founder

Valtech
Dmytro Kozlovskyy, Head of Legal & Partnership

SoftServe
Oleh Denys, Co-founder, Executive Vice President, Audit

Uklon
Serhii Hryshkov, CEO

Preply
Bohdan Krevskyi, Head of Finance

BlueBird
Bogdan Stankevich, Co-founder

LUN
Denys Sudilkovsky, CBBO