

Otokar Otomotiv ve Savunma Sanayi A.Ş.

Artificial Intelligence Ethical and Responsible Governance Policy

Table of Contents

1.PURPOSE AND SCOPE	3
2. DEFINITIONS	3
3. GENERAL PRINCIPLES.....	4
4. APPLICATION OF THE POLICY	5
4.1. Preliminary Assessment and Risk Classification	5
4.2. Framework for the Use of AI Systems	7
4.3. Audit and Periodic Reporting	9
4.4. Training and Awareness	9
6. REVISION HISTORY	10

1. PURPOSE AND SCOPE

The purpose of this Artificial Intelligence Ethical and Responsible Governance Policy (**the “Policy”**) is to establish the fundamental principles governing the ethical, safe, responsible, transparent and legally compliant development, procurement, integration, use, monitoring and decommissioning of artificial intelligence (**“AI”**) systems throughout their lifecycle (**the “AI Lifecycle”**) within Otokar Otomotiv ve Savunma Sanayi A.Ş. (**“Otokar”**).

This Policy has been developed in alignment with the Otokar Code of Ethics and applicable Compliance Policies and shall be reviewed periodically and updated as necessary considering evolving principles and standards applicable to AI systems, technological developments, regulatory changes and emerging needs.

All Otokar employees and executives are required to comply with this Policy. Otokar shall also expect its Business Partners to comply with this Policy to the extent applicable to the relevant party and/or transaction and shall take appropriate steps to promote such compliance.

2. DEFINITIONS

“AI Systems” means machine-based models, applications or services that process data in accordance with human-defined objectives and parameters to generate outputs.

“Artificial Intelligence (AI)” means software or systems designed to support human decision-making processes by generating outputs such as classifications, predictions, recommendations or content based on data, rules or a combination thereof.

“Business Partner” includes suppliers, distributors, dealers, authorized services and other third parties with whom the company has a business relationship and all kinds of representatives, subcontractors, consultants, etc. acting on behalf of the company, as well as their employees and representatives.

“Koç Group” means Koç Holding A.Ş., companies which are controlled directly or indirectly, jointly or individually by Koç Holding A.Ş. and the joint venture companies listed in its latest consolidated financial report.

“Lifecycle” means the process encompassing the development, procurement, integration, use, monitoring and decommissioning of AI Systems.

“Personal Data” means any information relating to an identified or identifiable natural person.

“Processing of Personal Data” means any operation performed on Personal Data, including collection, recording, storage, retention, alteration, reorganization, disclosure, transfer, acquisition, making available, classification or restriction of use, whether carried out wholly or partly by automated means or by non-automated means where the data forms part of a data filing system.

“Sensitive Personal Data” means Personal Data relating to race, ethnic origin, political opinions, philosophical beliefs, religion, sect or other beliefs, appearance and clothing, membership of associations, foundations or trade unions, health, sexual life, criminal convictions and security measures, as well as biometric and genetic data.

3. GENERAL PRINCIPLES

Within Otokar, the AI Lifecycle shall be governed in accordance with the following principles, based on a human-centric approach to the ethical, safe, responsible, transparent and legally compliant use of AI:

Legal and Regulatory Compliance: Full compliance with all applicable laws and regulations is a fundamental requirement in the development and use of AI Systems.

The use of AI Systems may involve the Processing of Personal Data at both the input and output stages. Accordingly, whenever information relating to an identified or identifiable natural person is processed, all applicable data protection and privacy laws must be observed. This principle requires compliance not only with the local laws of the jurisdiction in which the relevant company is established, but also, where AI services or products are offered in or directed to markets or consumers in other jurisdictions, with other applicable laws and regulations.

Under no circumstances may confidential information, inside information, trade secrets or Personal Data of a sensitive nature, whether or not classified as Sensitive Personal Data, be entered into or shared with external or publicly available AI Systems¹. Where a non-public AI System is used and the transfer of Personal Data is necessary, it must be ensured that such transfer is carried out in compliance with applicable data protection and privacy laws and this Policy.

Ethical Responsibility: AI technologies shall be designed, developed and used in accordance with the Otokar Code of Ethics and applicable Compliance Policies. In this context:

- AI Systems must not undermine fundamental rights and freedoms or produce adverse effects such as discrimination, bias or social exclusion.
- AI Systems developed or used within Otokar must be ethical, safe, responsible, transparent, legally compliant and consistent with the relevant Otokar’s Information Security Policy and the Otokar Artificial Intelligence Security Standards. Data sets used to train or otherwise support such systems must also be structured in a balanced manner consistent with the principles of diversity and inclusion.
- It must be recognized that output generated by AI Systems may be inaccurate, inconsistent, biased or misleading. Accordingly, output including text, code, images, reports and similar content must be reviewed for accuracy, up-to-dateness and legal compliance before being used in business processes.

¹ Explained in Section 4.2, “Framework for the Use of AI Systems.

- Outputs generated by AI Systems shall be subject to appropriate human oversight mechanisms commensurate with the applicable risk level. Human approval is mandatory for processes that have legal consequences, create financial impact, affect individual rights or are classified as high risk. Human oversight must remain the decisive factor in processes such as recruitment, promotion and customer communications where outcomes may adversely affect individuals. In low-risk operational workflows governed by predefined rules, AI Systems may be permitted to execute automated actions, provided that appropriate technical controls, monitoring and intervention mechanisms are in place.
- AI Systems must never be used to manipulate individual behavior, collect Personal Data without authorization, perform emotion recognition or social scoring, conduct remote biometric identification in public spaces, or otherwise infringe fundamental rights and freedoms.

Transparency: The purpose, scope and limitations of AI Systems must be clearly understandable to relevant users. The operation of the algorithm and the logical relationship between inputs and outputs should be traceable and explainable. AI-generated content must not be presented as human-generated content by concealing its origin. Users must be enabled to understand when an activity or process is supported by AI. Where appropriate, content generated by AI shall be clearly identified as such to users.

Accountability and Traceability: Users are accountable for the accuracy of all content they create, publish or use for business purposes, including materials generated by AI. Ownership, accountability and approval mechanisms must be clearly defined for each AI System. Model versions, data sources, intended use and system outputs must be documented in a manner that enables auditability where necessary, and traceability must be maintained through mechanisms such as logging. For third-party or closed AI Systems, a reasonable level of transparency and record-keeping shall be maintained based on the information and technical documentation made available by the provider.

Sustainability and Social Benefit: Otokar encourages the use of AI in ways that contribute to sustainability objectives and social benefit. Otokar supports the training of its stakeholders, children and young people regarding the ethical, safe, responsible and transparent use of AI Systems. Where appropriate, the sustainability impacts of AI Systems shall be measured and monitored, and energy efficiency and environmental impacts shall be considered when selecting and using AI solutions.

4. APPLICATION OF THE POLICY

The development, procurement and use of AI Systems within Otokar shall be conducted within an established accountability framework. Controls applicable before, during and after the development or use of AI Systems shall be based on the principles set out below.

4.1. Preliminary Assessment and Risk Classification

Before developing a new AI System (or a new product, process or similar solution incorporating AI) intended for enterprise-wide deployment or systematic integration into business processes, or before planning the widespread use of a new AI System in business processes, the relevant business unit shall conduct a preliminary assessment in consultation with the Otokar Legal and Compliance Department and Otokar Information Technology and Digital Transformation Leadership, in accordance with the standardized methodological approach applied across Koç Group, in order to ensure compliance with this Policy. The assessment shall consider the business need addressed by the AI System, the data on which it operates, the extent to which its output influence human decision-making, how inaccurate or inconsistent results will be identified and managed, and how necessary remediation or action plans will be implemented.

As a general principle, standardized AI applications designated by the department responsible for Information Technology shall be used across Otokar. Before using any AI System other than such standardized applications, employees must consult the Otokar Legal and Compliance Department and the Otokar Information Technology and Digital Transformation Leadership and obtain the required approvals following the Preliminary Assessment.

During the Preliminary Assessment, the AI System shall be classified² by risk level, considering its impacts and context of use. The classification shall be based on the potential consequences of AI use for human rights, decision-making processes and operations.

The risk levels are defined as follows:

Risk Level	Definition
Very High Risk (Prohibited)	Applications that pose a serious threat to society and systematically violate fundamental rights are strictly prohibited.
High Risk	Systems that directly affect individuals' fundamental rights and freedoms, safety or economic circumstances; whose erroneous outputs could have serious consequences; or that require specific authorization from regulatory authorities.
Medium Risk	Systems used for decision support or operational efficiency where the impact of erroneous outputs is limited.
Low Risk	Systems used for analysis, visualization or informational purposes whose outputs are non-critical.

The following control mechanisms are applied according to risk level:

Risk Level	Implementation and Control Process
Very High Risk	Use or deployment is prohibited under all circumstances.

² Under the Otokar Risk Management Methodology, Artificial Intelligence Risks are classified as Technology Risks within the Operational Risk category.

High Risk	The relevant business units, together with the Otokar Legal and Compliance Department and the Otokar Information Technology and Digital Transformation Leadership, shall prepare a Fundamental Rights and Impact Assessment. The assessment, together with identified risks and potential impacts, shall be submitted for approval to the General Manager and/or the relevant committee. If approved, the rationale for use, the relevant risk assessment report and the mitigating measures shall be reported to the Koç Holding Legal and Compliance Department and the Information Technology Coordination Department prior to go-live. The process may be subject to internal audit where necessary.
Low and Medium Risk	The assessment and approval process shall be managed by the relevant business unit in coordination with the Otokar Information Technology and Digital Transformation Leadership; the opinion of the Otokar Legal and Compliance Departments shall be obtained where necessary.

The Preliminary Assessment also determines the technical environment in which the AI System may be used. This framework is further described in the “Framework for the Use of AI Systems” section below.

4.2. Framework for the Use of AI Systems

The use of AI Systems must be fully compliant with the Otokar Code of Ethics and Compliance Policies, the relevant company’s Information Security Policy, the Otokar Artificial Intelligence Security Standards and this Policy.

AI processes accessed, used or developed by Otokar shall be governed in accordance with the core security principles set out in the Artificial Intelligence Security Standard.

Appropriate technical security measures shall be implemented for AI Systems, including data protection, access controls and safeguards against common threats. AI solutions shall, to the extent practicable, be subject to security testing and supported by controls designed to mitigate misuse risks. These technical measures are further detailed in the Artificial Intelligence Security Standard.

The technical infrastructure used for the development, hosting and data processing of AI Systems determines the applicable security level and control framework. Accordingly, the required security assessments must also be conducted as part of the Preliminary Assessment. AI Systems shall be assessed under the following three categories:

System Type	Definition
Secure AI Systems	Systems whose development, server hosting, management and data processing are conducted within Otokar’s information technology infrastructure and security policies. These systems are the preferred option where Personal Data is processed.

System Type	Definition
Approved AI Systems	AI applications authorized for use following an assessment of security and infrastructure controls, Personal Data protection, ethical compliance, contractual obligations and business purpose. The assessment shall be conducted jointly by the relevant business unit, the Otokar Legal and Compliance Department and the Otokar Information Technology and Digital Transformation Leadership.
Externally Sourced or Publicly Available AI Systems	Systems operating outside the direct control of Otokar where data processing activities are not fully subject to Otokar oversight. Such systems may only be used for general-purpose, low-risk activities that do not require data sharing. The transfer of Personal Data, classified or confidential information, trade secrets or Otokar internal information to such platforms is strictly prohibited. This prohibition also applies to AI Agents used as components of AI Systems that can execute automated actions in pursuit of predefined objectives.

Before procuring an externally sourced or publicly available AI System, or software incorporating such capabilities, technical documentation must be requested from the relevant Business Partner, including information on the source of training data, model bias testing results and commitments regarding legal and regulatory compliance. No procurement may proceed until this assessment has been completed and the required Business Partner Risk Approval has been obtained. Contracts with the Business Partner must also contain appropriate protective provisions addressing liability and indemnification for risks arising from the systems or software provided, including data breaches, algorithmic discrimination and intellectual property infringement.

For general-purpose and publicly available AI Systems, it should be recognized that data processing activities may not be technically traceable with full transparency and that visibility into processing by sub-processors may be limited. Contractual commitments should therefore not be regarded as sufficient safeguards on their own. Data classification rules, the principle of data minimization and enterprise security controls must be applied as primary safeguards. Intellectual property ownership and commercial-use restrictions must also be separately assessed for code, text, images, designs and similar outputs generated by AI Systems. Before such outputs are used in commercial products, customer deliverables or intellectual property filings, the necessary review must be conducted with Otokar Legal and Compliance Department and/or Otokar Intellectual Property Group.

Before using any AI System other than standardized applications, employees must consult the Otokar Legal and Compliance Department and the Otokar Information Technology and Digital Transformation Leadership and obtain the required approvals following the Preliminary Assessment. Depending on the intended use and risk level, the Preliminary Assessment may include input from relevant Legal, Data Privacy, Intellectual Property, Commercial and technical teams.

4.3. Audit and Periodic Reporting

Preliminary assessments relating to AI Systems approved for development or use shall be subject to ongoing oversight and periodic reporting by the Otokar Legal and Compliance Department and the Otokar Information Technology and Digital Transformation Leadership.

All content generated by Generative AI systems—including text, code, images, reports and similar materials—must be reviewed before being used in business processes or published. Unverified AI outputs must not be treated as definitive fact or as representing the company’s position and must not be shared with third parties. Otokar Information Technology and Digital Transformation Leadership are responsible for designing and implementing the necessary control mechanisms for AI use.

Otokar Information Technology and Digital Transformation Leadership, the effectiveness of AI use processes, the integrity of audit trails and the operating effectiveness of controls shall be assessed, where necessary, as part of risk-based audit plans. Corrective actions relating to identified non-compliance or control deficiencies shall be planned and implemented by the relevant functions, and the Otokar Information Technology and Digital Transformation Leadership shall monitor completion of such actions. Where appropriate, the AI governance framework may also be subject to independent assessment and review for alignment with international standards.

Human review and assessment shall be provided, where necessary, for AI-assisted decisions that have a significant impact on individuals.

AI Systems deployed in production shall be subject to periodic technical testing by the Otokar Information Technology and Digital Transformation Leadership to identify performance degradation, Model Drift and deterioration in data quality over time. Models found to have fallen below their baseline performance criteria should be immediately withdrawn from use for retraining or review. AI Systems used in production shall also be reviewed at appropriate intervals for fairness and bias.

4.4. Training and Awareness

Otokar is committed to continuously enhancing employee awareness to support the ethical, safe, responsible, transparent and legally compliant use of AI. In this context, individuals designated by the Otokar Information Technology and Digital Transformation Leadership shall receive regular reminders of their individual responsibilities and periodic training necessary to ensure the ethical, safe, responsible, transparent and legally compliant use of AI Systems. Business Partners shall also be encouraged to participate in such training. Training content and awareness initiatives shall be tailored to employees’ roles and responsibilities, and training may be made mandatory for certain roles or functions before new or updated AI Systems are deployed.

Awareness encompasses not only knowledge but also behavioral accountability. Employees are expected to stop the relevant process and contact the Otokar Legal and Compliance Department or the Otokar Information Technology and Digital Transformation Leadership if they encounter circumstances in the use of AI Systems that appear suspicious, risky or raise ethical concerns.

5. AUTHORITY AND RESPONSIBILITIES

All employees and directors of Otokar are responsible for complying with this Policy, implementing and supporting the Otokar's procedures and controls in accordance with the requirements of this Policy. Otokar also expects and takes necessary steps to ensure that all its Business Partners, to the extent applicable, comply with and/or act in accordance with this Policy.

If there is a discrepancy between the local regulations, applicable in the countries where Otokar operates, and this Policy, the stricter of the two shall prevail, unless such practice is in violation of the relevant local laws and regulations.

If you become aware of any action that you believe is inconsistent with this Policy, the applicable law or the Otokar Code of Ethics, you may seek guidance or report the incident to your line manager. Alternatively, you may report the incident to Koç Group's Ethics Hotline via the following link: "koc.com.tr/hotline"

Otokar employees may contact the Legal and Compliance Department of Otokar for their questions regarding this Policy and its application. Violation of this Policy may result in significant disciplinary actions including dismissal. If this Policy is violated by third parties, their contracts may be terminated.

6. REVISION HISTORY

This Policy takes effect on 25.09.2026 as of the date approved by the Board of Directors and will be maintained by the Otokar Legal and Compliance Department.

Revision	Date	Comment