RESPONSIBLE ARTIFICIAL INTELLIGENCE USE POLICY IN THE KRKA GROUP

1 Purpose and scope

The Responsible Artificial Intelligence Use Policy in the Krka Group (hereinafter: the Policy) applies to the controlling company Krka, tovarna zdravil, d. d., Novo mesto, and its subsidiaries, which together form the Krka Group (hereinafter: Krka). It applies to all employees and all processes at Krka.

The Policy establishes the principles for managing artificial intelligence systems throughout their entire life cycle and provides the foundation for the further development of the responsible use of artificial intelligence at Krka. For internal purposes, we have established rules and standard operating procedures governing individual aspects of use, including information security, confidentiality and the protection of trade secrets.

We are committed to the responsible, ethical and safe development, procurement, implementation and use of artificial intelligence in accordance with applicable national and international legal and regulatory requirements, guidelines and recognised standards. We also take into account evolving regulatory requirements and expectations, including the revision of Annex 11 to the EU GMP Guidelines (Computerised Systems), the new Annex 22 to the EU GMP Guidelines (Artificial Intelligence), and the revision of Chapter 4 of EudraLex Volume 4 (Documentation), as well as recognised standards for information security and artificial intelligence management systems.

2 Classification of artificial intelligence solutions

Based on the degree of customisation, integration into business processes and autonomy, we classify artificial intelligence solutions into the following groups.

a) **Commercial general-purpose solutions.** These solutions are obtained from commercial providers. We use them in their original form, without additional internal development or adaptation to the specific needs of Krka's processes (e.g. Microsoft Copilot).
b) **Customised hybrid solutions.** These solutions are based on existing platforms or commercial models and have been customised, upgraded or extended at Krka, for example with proprietary data, RAG architectures (Retrieval-Augmented Generation), personal artificial intelligence agents or specific business logic. Such solutions are partially adapted to internal business requirements.
c) **Specialised solutions.** These solutions are developed internally or in cooperation with external providers and are specifically tailored to support Krka's internal business processes. They do not operate autonomously and are used solely as decision-support tools, with oversight ensured through human involvement in decision-making (Human-in-the-Loop, HITL).
d) **Specialised autonomous solutions.** These solutions are integrated into internal business processes and may operate autonomously, without direct human approval of individual decisions or actions. Due to their higher level of risk, they are subject to the strictest requirements for risk assessment, testing, validation and continuous monitoring throughout their life cycle. The use of autonomous dynamic artificial

intelligence models, whether deterministic or non-deterministic, to perform or approve GxP-critical tasks is not permitted.

3 Principles

We are committed to the responsible, ethical and safe development, procurement, implementation and use of artificial intelligence. The following principles guide us in fulfilling this commitment.

3.1 Human-centred artificial intelligence

Artificial intelligence systems at Krka support employees in their work and do not replace their professional judgement, creativity or responsibility. A human always remains accountable for decisions, actions and outcomes supported by artificial intelligence, with appropriate human oversight ensured for important decisions. Appropriately qualified employees remain involved in critical decisions and can review, intervene in, override or stop artificial intelligence recommendations or actions.

3.2 Safety, reliability and quality

Before implementation and during use, we assess artificial intelligence systems for suitability, reliability, accuracy and effectiveness. We have established monitoring mechanisms to identify performance degradation, model drift, undesirable behaviour and other issues that could affect reliability or business outcomes. Where necessary, we implement control measures, including restricting, updating or withdrawing a system from use.

3.3 Transparency

When using artificial intelligence, we ensure an appropriate level of transparency based on the intended use, risk level and technical feasibility. Where appropriate and technically feasible, we inform users that they are using or interacting with artificial intelligence systems; clearly label content generated by artificial intelligence; clearly distinguish between results generated by or with the support of artificial intelligence and results produced by humans; and provide relevant stakeholders with appropriate information about decisions in which artificial intelligence was involved.

3.4 Fairness and non-discrimination

In the development, procurement, implementation and use of artificial intelligence, we prevent unacceptable bias, discrimination and other forms of unequal treatment. We regularly assess systems for potential adverse effects on individuals or groups and, where necessary, implement measures to mitigate them. Artificial intelligence systems must support fair, objective and responsible decision-making.

3.5 Privacy and personal data protection

Personal data and other sensitive information are processed only for lawful purposes and with appropriate safeguards and control mechanisms in place.

We design and use artificial intelligence systems in accordance with applicable personal data protection legislation and recognised privacy principles. Data used to train, test, operate or improve these systems must be collected, processed, stored and protected responsibly and in accordance with legal requirements.

3.6 Data integrity and governance

Data used to train, test, operate and monitor artificial intelligence systems are managed throughout their life cycle within Krka's data governance system, taking into account the principles of confidentiality, integrity and availability, as well as the ALCOA+ principles. Source data and associated metadata remain the reference records, while results generated by artificial intelligence are treated as processed data. The link to the source data is maintained so that the origin of each result can be reconstructed.

For records processed by artificial intelligence systems, we define ownership, classification, confidentiality level, GxP relevance and retention period. The audit trail records who changed what, when and why, and equivalent requirements also apply to data, models and services provided by third parties.

3.7 Cybersecurity and confidentiality

We integrate cybersecurity into the entire life cycle of artificial intelligence systems. Cybersecurity is managed in accordance with the Information Security Policy in the Krka Group, which establishes overarching principles for protecting Krka's information assets and managing information and cybersecurity risks.

We implement appropriate technical and organisational measures to protect artificial intelligence systems, related data and supporting infrastructure against unauthorised access, manipulation, misuse, disclosure or cyber threats.

Security assessments, monitoring activities and risk management procedures contribute to ensuring the reliability and trustworthy operation of these systems.

Internal and confidential data are processed only in environments under our control, either in our own infrastructure (on-premises) or, for example, in Krka's Microsoft 365 environment (M365 tenant).

3.8 Accountability, governance and monitoring

Clear roles, responsibilities and procedures are defined for assessing, approving, monitoring and overseeing artificial intelligence initiatives. The Management Board member responsible for artificial intelligence and the Strategic Artificial Intelligence Group are responsible for implementing this Policy. Together, they address artificial intelligence-related projects,

regulatory requirements, potential risks and the practical aspects of implementing and using artificial intelligence at Krka.

3.9 Clearly defined scope and responsible use

Artificial intelligence systems are used exclusively for approved, lawful and clearly defined purposes. Before implementation, the intended use, limitations and operating boundaries are defined, and users must professionally and critically assess artificial intelligence outputs before use. Significant changes to models, data sources or integrations, including supplier updates, must be assessed for their impact before use and appropriately tested according to the level of risk.

Users are expected to critically evaluate outputs generated by artificial intelligence and assess them from a professional perspective before use.

3.10 Prohibited uses of artificial intelligence

Krka does not develop, implement or use artificial intelligence systems for purposes prohibited by law, particularly where they involve manipulation, exploitation of vulnerable individuals, social scoring, unlawful biometric surveillance or other prohibited practices.

3.11 Training and awareness

Employees who develop, procure, manage or use artificial intelligence systems receive appropriate training and awareness according to their role, responsibility and level of interaction with these systems. Programmes include: responsible and ethical use of artificial intelligence; information and cybersecurity; privacy and personal data protection requirements; identification and mitigation of artificial intelligence-related risks; responsibilities for ensuring human oversight; applicable legal and regulatory obligations; data integrity principles (ALCOA+) and good documentation practices; and requirements applicable to artificial intelligence used in GxP-regulated and other regulated processes.

Training is regularly reviewed and updated in line with developments in technology, regulations and professional practice.

3.12 Stakeholder rights and options for reporting potential incidents

We enable stakeholders to raise concerns, report incidents or request additional explanations regarding the use of artificial intelligence. All reports are handled within the established incident and deviation management procedures.

Stakeholders affected by the results may raise concerns or request an explanation by email at Compliance.officer@krka.biz.

3.13 Artificial intelligence in GxP-regulated processes

Artificial intelligence systems that may directly affect patient safety, the quality of Krka's products or data integrity are subject to additional requirements proportionate to the risk and aligned with Annex 11 to the EU GMP Guidelines (Computerised Systems) and Annex 22 (Artificial Intelligence).

- Before acceptance testing, we define and approve the intended use, input data and limitations, as well as testing and acceptance criteria. Performance must be at least equivalent to that of the process replaced by the model.
- Testing is conducted in accordance with an approved test plan using representative test data independent of the data used for development, training and validation. Results, deviations, and the characteristics and confidence level associated with model outputs are documented and reviewed.
- During use, the model, system and process are subject to change and configuration control. We monitor model performance and input data drift and maintain records of human reviews, records and reports approved by the Quality Assurance department that affect the assessment of product quality.

Human oversight does not replace required validation. The scope of validation is determined based on the intended use, GxP impact and documented risk assessment.

4 Final provisions

The Policy was adopted by the Management Board of Krka, tovarna zdravil, d. d., Novo mesto, at its 13th regular meeting on 21 October 2026.

The Policy is a public document and is published on Krka's website. It is reviewed and, where necessary, updated at least once every five years and upon significant changes to the applicable legal framework. All amendments and supplements must be approved by the Management Board.