POLITIKA ODGOVORNE UPORABE UMETNE INTELIGENCE V SKUPINI KRKA

1 Namen in področje uporabe

Politika odgovorne uporabe umetne inteligence v skupini Krka (v nadaljevanju Politika) velja za obvladujočo družbo Krka, tovarna zdravil, d. d., Novo mesto in njene odvisne družbe, ki skupaj sestavljajo Skupino Krka (v nadaljevanju Krka). Velja za vse zaposlene in vse procese v Krki.

Politika določa načela upravljanja sistemov umetne inteligence v njihovem celotnem življenjskem ciklu in je temelj za nadaljnji razvoj odgovorne uporabe umetne inteligence v Krki. Za interne potrebe imamo vzpostavljena pravila in standardne operativne postopke, ki urejajo posamezne vidike uporabe, vključno z informacijsko varnostjo, zaupnostjo in varstvom poslovnih skrivnosti.

Zavezani smo odgovornemu, etičnemu in varnemu razvoju, nabavi, uvajanju in uporabi umetne inteligence v skladu z veljavnimi nacionalnimi in mednarodnimi zakonskimi in regulativnimi zahtevami, smernicami in priznanimi standardi. Pri tem upoštevamo tudi spreminjajoče se regulativne zahteve in pričakovanja, vključno s spremembo Priloge 11 smernic EU GMP (računalniško podprti sistemi), novo Prilogo 22 smernic EU GMP (umetna inteligenca) in spremembo 4. poglavja 4. zvezka EudraLex (dokumentacija), ter priznane standarde za informacijsko varnost in sisteme upravljanja umetne inteligence.

2 Razvrstitev rešitev umetne inteligence

Glede na stopnjo prilagojenosti, vključenosti v poslovne procese in avtonomnosti rešitve umetne inteligence razvrščamo v naslednje skupine.

a) **Komercialne rešitve za splošne namene.** Te rešitve pridobimo od komercialnih ponudnikov. Uporabljamo jih v njihovi prvotni obliki, brez dodatnega internega razvoja ali prilagajanja posebnim potrebam Krkinih procesov (npr. Microsoft Copilot).
b) **Prilagojene hibridne rešitve.** Te rešitve temeljijo na obstoječih platformah ali komercialnih modelih, v Krki pa so bile prilagojene, nadgrajene ali razširjene, na primer z lastnimi podatki, arhitekturami RAG (generiranje s pomočjo pridobivanja podatkov, angl. *Retrieval-Augmented Generation*), osebnimi umetno inteligenčnimi agenti ali posebno poslovno logiko. Tovrstne rešitve so delno prilagojene internim poslovnim zahtevam.
c) **Specializirane rešitve.** Te rešitve so razvite interno ali v sodelovanju z zunanjimi ponudniki in so posebej prilagojene za podporo Krkinim internim poslovnim procesom. Ne delujejo avtonomno in se uporabljajo zgolj kot orodje za podporo pri odločanju, pri čemer je nadzor zagotovljen z vključevanjem človeka v odločanje (angl. *Human-in-the-Loop*, HITL).
d) **Specializirane avtonomne rešitve.** Te rešitve so vključene v interne poslovne procese in lahko delujejo avtonomno, brez neposredne človeške odobritve posameznih odločitev ali dejanj. Zaradi višje ravni tveganja zanje veljajo najstrožje zahteve glede ocenjevanja tveganj, testiranja, validacij in stalnega spremljanja v celotnem življenjskem ciklu. Uporaba avtonomnih dinamičnih modelov umetne inteligence, ne

glede na to, ali so deterministični ali ne deterministični, za izvajanje ali odobravanje nalog, kritičnih z vidika GxP, ni dovoljena.

3 Načela

Zavezani smo odgovornemu, etičnemu in varnemu razvoju, nabavi, uvajanju in uporabi umetne inteligence. Pri uresničevanju te zaveze nas vodijo naslednja načela.

3.1 K človeku usmerjena umetna inteligenca

Sistemi umetne inteligence v Krki podpirajo delo zaposlenih ter ne nadomeščajo njihove strokovne presoje, ustvarjalnosti in odgovornosti. Za odločitve, dejanja in rezultate, podprte z umetno inteligenco, vedno odgovarja človek, pri čemer je pri pomembnih odločitvah zagotovljen ustrezen človeški nadzor. Pri kritičnih odločitvah ostajajo vključeni ustrezno usposobljeni zaposleni, ki lahko priporočila oziroma dejanja umetne inteligence pregledajo, vanje posežejo, jih razveljavijo ali ustavijo.

3.2 Varnost, zanesljivost in kakovost

Sisteme umetne inteligence pred uvedbo in med uporabo ocenjujemo glede njihove primernosti, zanesljivosti, točnosti in učinkovitosti. Vzpostavili smo mehanizme spremljanja za prepoznavanje poslabšanja učinkovitosti delovanja, odklonov v delovanju modelov, neželenega vedenja in drugih težav, ki bi lahko vplivale na zanesljivost ali poslovne rezultate. Po potrebi izvajamo kontrolne ukrepe, vključno z omejitvijo, posodobitvijo ali umikom sistema iz uporabe.

3.3 Preglednost

Pri uporabi umetne inteligence zagotavljamo ustrezno stopnjo preglednosti glede na namen uporabe, raven tveganja in tehnične možnosti. Kadar je to primerno in tehnično izvedljivo, uporabnike obveščamo, da uporabljajo sisteme umetne inteligence oziroma z njimi sodelujejo; vsebine, ki jih ustvari umetna inteligenca, jasno označujemo; jasno razlikujemo med rezultati, ki so bili ustvarjeni z umetno inteligenco ali z njeno podporo, in rezultati, ki jih je ustvaril človek; relevantnim deležnikom zagotavljamo ustrezne informacije o odločitvah, pri katerih je sodelovala umetna inteligenca.

3.4 Pravičnost in nediskriminacija

Pri razvoju, nabavi, uvajanju in uporabi umetne inteligence preprečujemo nedopustno pristranskost, diskriminacijo in druge neenake obravnave. Sisteme redno preverjamo glede morebitnih negativnih vplivov na posameznike ali skupine ter po potrebi izvajamo ukrepe za njihovo zmanjšanje. Sistemi umetne inteligence morajo podpirati pravično, objektivno in odgovorno odločanje.

3.5 Zasebnost in varstvo osebnih podatkov

Osebni podatki in druge občutljive informacije se obdelujejo le za zakonite namene ter ob uporabi ustreznih zaščitnih ukrepov in nadzornih mehanizmov.

Sisteme umetne inteligence načrtujemo in uporabljamo v skladu z veljavno zakonodajo o varstvu osebnih podatkov in priznanimi načeli varstva zasebnosti. Podatki, ki se uporabljajo za učenje, testiranje, delovanje ali izboljševanje teh sistemov, morajo biti zbrani, obdelani, shranjeni in varovani odgovorno ter v skladu z zakonskimi zahtevami.

3.6 Celovitost in upravljanje podatkov

Podatke, ki se uporabljajo za učenje, testiranje, delovanje in spremljanje sistemov umetne inteligence, v celotnem življenjskem ciklu upravljamo v okviru Krkinega sistema upravljanja podatkov, pri čemer upoštevamo načela zaupnosti, celovitosti in razpoložljivosti ter načela ALCOA+. Izvorni podatki in pripadajoči metapodatki ostajajo referenčni zapisi, rezultate, ki jih ustvari umetna inteligenca, pa obravnavamo kot obdelane podatke. Povezava z izvornimi podatki se ohranja tako, da je izvor posameznega rezultata mogoče rekonstruirati.

Za zapise, ki jih obdelujejo sistemi umetne inteligence, določamo lastništvo, razvrstitev, stopnjo zaupnosti, pomen za GxP in obdobje hrambe. Revizijska sled beleži, kdo je kaj spremenil, kdaj in zakaj, enakovredne zahteve pa veljajo tudi za podatke, modele in storitve, ki jih zagotavljajo tretje osebe.

3.7 Kibernetska varnost in zaupnost

Področja kibernetske varnosti vključujemo v celoten življenjski cikel sistemov umetne inteligence. Kibernetsko varnost upravljamo v skladu s **Politiko informacijske varnosti v skupini Krka**, ki določa krovna načela za varovanje Krkinih informacijskih sredstev ter obvladovanje tveganj informacijske in kibernetske varnosti.

Za zaščito sistemov umetne inteligence, z njimi povezanih podatkov in podporne infrastrukture pred nepooblaščenim dostopom, manipulacijo, zlorabo, razkritjem ali kibernetskimi grožnjami izvajamo ustrezne tehnične in organizacijske ukrepe.

Varnostne ocene, dejavnosti spremljanja in postopki obvladovanja tveganj prispevajo k zagotavljanju zanesljivosti in zaupanja vrednega delovanja teh sistemov.

Interne in zaupne podatke obdelujemo samo v okoljih, ki jih nadzorujemo, bodisi v lastni infrastrukturi (angl. on-premises) bodisi, na primer, v Krkinem okolju Microsoft 365 (M365 tenant).

3.8 Odgovornost, upravljanje in spremljanje

Za upravljanje umetne inteligence so določene jasne vloge, odgovornosti in postopki za ocenjevanje, odobravanje, spremljanje in nadzor pobud na področju umetne inteligence. Za izvajanje te politike sta odgovorna član uprave, pristojen za umetno inteligenco, in strateška skupina za umetno inteligenco. Skupaj obravnavata projekte, povezane z umetno inteligenco,

regulativne zahteve, morebitna tveganja ter praktične vidike uvajanja in uporabe umetne inteligence v Krki.

3.9 Jasno opredeljeno področje uporabe in odgovorna uporaba

Sistemi umetne inteligence se uporabljajo izključno za odobrene, zakonite in jasno opredeljene namene. Pred uvedbo se opredelijo predvidena uporaba, omejitve in meje delovanja, uporabniki pa morajo rezultate umetne inteligence pred uporabo strokovno in kritično presoditi. Pomembne spremembe modelov, virov podatkov ali integracij, vključno s posodobitvami dobaviteljev, je treba pred uporabo oceniti z vidika njihovega vpliva in ustrezno preizkusiti glede na raven tveganja.

Od uporabnikov pričakujemo, da rezultate, ki jih ustvari umetna inteligenca, pred uporabo kritično ovrednotijo in presodijo s strokovnega vidika.

3.10 Prepovedana uporaba umetne inteligence

Krka ne razvija, uvaja ali uporablja sistemov umetne inteligence za namene, ki jih prepoveduje zakonodaja, zlasti če vključujejo manipulacijo, izkoriščanje ranljivih posameznikov, družbeno ocenjevanje, nedovoljen biometrični nadzor ali druge prepovedane prakse.

3.11 Usposabljanje in ozaveščanje

Zaposlene, ki razvijajo, nabavljajo, upravljajo ali uporabljajo sisteme umetne inteligence, ustrezno usposabljamo in ozaveščamo glede na vlogo, odgovornost in stopnjo interakcije s temi sistemi. Programi vključujejo: odgovorno in etično uporabo umetne inteligence; informacijsko in kibernetsko varnost; zahteve glede zasebnosti in varstva osebnih podatkov; prepoznavanje in zmanjševanje tveganj, povezanih z umetno inteligenco; odgovornosti pri zagotavljanju človeškega nadzora; veljavne zakonske in regulativne obveznosti; načela celovitosti podatkov (ALCOA+) in dobre dokumentacijske prakse; zahteve, ki veljajo za umetno inteligenco, uporabljeno v procesih, reguliranih z GxP, in drugih reguliranih procesih.

Usposabljanja redno pregledujemo in posodabljamo glede na razvoj tehnologij, predpisov in strokovne prakse.

3.12 Pravice deležnikov in možnosti za prijavo morebitnih incidentov

Deležnikom omogočamo, da izrazijo pomisleke, prijavijo incidente ali zaprosijo za dodatna pojasnila glede uporabe umetne inteligence. Vse prijave obravnavamo v okviru vzpostavljenih postopkov za upravljanje incidentov in odklonov.

Deležniki, na katere se rezultati nanašajo, lahko izrazijo pomisleke ali zaprosijo za pojasnilo prek e-naslova Compliance.officer@krka.biz.

3.13 Umetna inteligenca v procesih, reguliranih z GxP

Za sisteme umetne inteligence, ki lahko neposredno vplivajo na varnost pacientov, kakovost Krkinih izdelkov ali celovitost podatkov, veljajo dodatne zahteve, sorazmerne s tveganjem ter skladne s Prilogo 11 smernic EU GMP (računalniško podprti sistemi) in Prilogo 22 (umetna inteligenca).

- Pred sprejemnim testiranjem opredelimo in odobrimo predvideno uporabo, vhodne podatke in omejitve ter merila testiranja in sprejemljivosti. Učinkovitost delovanja mora biti najmanj enaka učinkovitosti procesa, ki ga model nadomešča.
- Testiranje poteka v skladu z odobrenim načrtom testiranja in z uporabo reprezentativnih testnih podatkov, neodvisnih od podatkov, uporabljenih pri razvoju, učenju in validaciji. Rezultate, odklone ter značilnosti in stopnjo zaupanja, povezane z rezultati modela, dokumentiramo in pregledamo.
- Med uporabo so model, sistem in proces predmet nadzora sprememb in konfiguracij. Spremljamo učinkovitost delovanja modela in odklone vhodnih podatkov, vodimo evidence človeških pregledov, zapisov in poročil, ki jih je odobril oddelek za zagotavljanje kakovosti in ki vplivajo na oceno kakovosti izdelka.

Človeški nadzor ne nadomešča zahtevane validacije. Obseg validacije se določi glede na predvideni namen uporabe, vpliv na GxP in dokumentirano oceno tveganja.

4 Končne določbe

Politiko je sprejela uprava Krke, tovarne zdravil, d. d., Novo mesto na 13. redni seji dne 21. 10. 2026.

Politika je javni dokument in je objavljena na Krkini spletni strani. Pregleda in po potrebi posodobi se najmanj enkrat na pet let ter ob pomembnih spremembah veljavnega pravnega okvira. Vse spremembe in dopolnitve mora odobriti uprava.