

PETERKA PARTNERS

YOUR CEE LAW FIRM

Technická normalizácia v umelej inteligencii

JUDr. Michal Rampášek

04.04.2024

Riadenie AI (Governance)



Zdroj: <https://www.responsible.ai>

Prečo používať technické normy v AI?

- Aktuálny stav *lege artis* a najlepšej praxe (*best practice*)
- Produkty, služby, procesy, materiály, subjekty a systémy manažérstva
- Dobrovoľnosť (nezáväznosť)
- Prostriedky na vyhodnotenie súladu s právnymi predpismi
ďalšie výhody pri dodržiavaní týchto noriem
- Certifikovateľné a auditovateľné (001)

Normalizačné orgány

- Celosvetovo pôsobiace medzinárodné normalizačné orgány:



- Európske normalizačné organizácie:



- Národné normalizačné orgány/
národné komitáty:



ÚRAD PRE NORMALIZÁCIU,
METROLÓGIU A SKÚŠOBNÍCTVO
SLOVENSKEJ REPUBLIKY

afnor

Francúzsko

DIN

Nemecko

DS
DANSK STANDARD

Dánsko

.....



Zdroj: <https://www.normoff.gov.sk/stranka/138/zakladne-vzdelavanie-o-technickej-normalizacii/?csrt=3100382847623563812>

Medzinárodné normy v AI

- Technická komisia ISO/IEC JTC 1/SC 42

Základné normy	Procesné normy	Normy merania	Normy výkonu
ISO/IEC 22989:2022	ISO/IEC 42001:2023 <i>(STN v procese)</i>	ISO/IEC TS 4213:2022	IEEE 2937-2022
ISO/IEC 23053:2022	ISO/IEC 38507:2022	ISO/IEC TR 24027:2021	
	ISO/IEC 23894:2023	ISO/IEC 24029:2021 (Part 1 a Part 2)	
	ISO/IEC 8183:2023	ISO/IEC 25059:2023	

ISO/IEC 42001:2023 Information technology. Artificial intelligence. Management system

- Poskytuje návod na vytvorenie, zavedenie, udržiavanie a neustále zlepšovanie systému manažérstva (***AI Management System, AIMS***).
- Pre organizácie všetkých veľkostí poskytuje požiadavky a usmernenia na implementáciu.
- Porovnanie s ISO 9001 a ISO/IEC 27001
- Príloha A (opatrenia na ošetrovanie rizík) a Príloha B (návod na implementáciu opatrení z prílohy A).
- Certifikovateľná a auditovateľná.
- Prebieha preklad a proces prevzatia do sústavy STN
- Porovnanie s NIST Rámcom riadenia rizík v oblasti AI (AI RMF)

ISO/IEC 23894:2023 Information technology. Artificial intelligence. Guidance on risk management

- Opisuje procesy integrácie a implementácie riadenia rizík v oblasti AI.
- Zrkadlí štruktúru ISO 31000:2018
- Jasnejšie zameranie na riziko odlišuje ISO/IEC 23894 od ISO/IEC 42001.
- 3 základné časti – Článok 4 (Princípy), článok 5 (Rámec) a článok 6 (Procesy)
- Mapovanie AI RMF 1.0 k norme ISO/IEC 23894 (články 5 a 6)



Európska normalizácia a AI

- Európske normy (EN) a Harmonizované normy (vyhlásené v Úradnom vestníku EÚ)
- Vykonávacie rozhodnutie Komisie C(2023)3215 zo dňa 22. mája 2023 o žiadosti na normalizáciu pre 10 oblastí
- Deadline: 30. apríl 2025 vs uplatňovanie Nariadenia o AI (2026)
- **Technický výbor CEN-CENELEC JTC21 pre AI (CEN/CLC/JTC 21 Work programme)**

Prijaté:	V procese:
<ul style="list-style-type: none">✓ EN ISO/IEC 22989:2023 (ISO/IEC 22989:2022)✓ EN ISO/IEC 23053:2023 (ISO/IEC 23053:2022)✓ EN ISO/IEC 23894:2024 (ISO/IEC 23894:2023)✓ CEN/CLC ISO/IEC/TR 24027:2023✓ CEN/CLC ISO/IEC/TR 24029-1:2023	<ul style="list-style-type: none">○ Systém manažérstva AI (ISO/IEC 42001)○ Posudzovanie zhody AI○ Dôveryhodnosť AI○ Požiadavky na kompetencie pre odborníkov v oblasti etiky AI○ Presnosť spracovanie prirodzeného jazyka○ Zelená a udržateľná AI○ Logovanie systémov AI

Normy a Nariadenie o AI

- Recitály č. 117 a č. 121
- *Súlاد s európskou harmonizovanou normou by mal poskytovateľom poskytnúť predpoklad zhody.*
- *Normalizácia by mala zohrávať kľúčovú úlohu pri poskytovaní technických riešení poskytovateľom na zabezpečenie súladu s týmto nariadením ...*
- *Dodržiavanie harmonizovaných noriem ... by malo byť pre poskytovateľov prostriedkom na preukázanie zhody s požiadavkami tohto nariadenia.*

Prezumpcia zhody

- Článok 40 (Harmonizované normy a normalizačné produkty)
- **Vysokorizikové systémy AI alebo systémy AI na všeobecné účely (GPAI)**, ktoré sú v zhode s harmonizovanými normami alebo ich časťami, na ktoré boli uverejnené odkazy v Úradnom vestníku Európskej únie, **sa považujú za systémy, ktoré sú v zhode s požiadavkami stanovenými v Nariadení o AI, a to v rozsahu, v akom sa tieto normy vzťahujú na uvedené požiadavky alebo povinnosti.**
- Článok 41 (Spoločné špecifikácie)
- Vykonávacie akty Komisie v prípade ak nemožno použiť harmonizované normy

Mimoeurópska technická normalizácia AI

USA	GB	Čína
NIST	BSI	TC260
Výkonný príkaz (<i>Executive order</i>) prezidenta USA o bezpečnej, chránenej a dôveryhodnej AI (2023) AI Risk Management Framework, NIST AI 100-1, pre generatívnu AI	BS ISO/IEC 42001:2023 Information technology. Artificial intelligence Management system	Biela kniha o štandardizácii bezpečnosti AI (2023) Základné požiadavky na bezpečnosť služieb generatívnej AI (návrh, 2023)



**Thank you
for your attention**

rampasek@peterkapartners.sk

Czech Republic Slovakia Ukraine Bulgaria
Poland Romania Hungary Croatia