Az AI alkalmazásának szakmai és szabályozási keretei

KKV digitalizáció: Lehetőség vagy versenykényszer?

Nagy Roland
HTEnet


Virtuális és fizikai környezet
Információ
AI „blackbox”
Személyek (és adataik)


Virtuális és fizikai környezet
Információ
AI „blackbox”
Személyek (és adataik)
Kockázatok

Kockázatok széles spektruma

Adatszivárgás

Anomáliák az informatikai rendszerekben

Törölt fájlok

Jelszó a promptban

Szerzői jogi jogsértés

Kritikus infrastruktúrának adott téves utasítás

Túlzott bizalom

Megfelelési rés

Reputációs kár

Emberi felügyelet hiánya

Diszkriminatív szöveg

Nem létező források

Szakértelem leépülése

Kényes meeting rögzítése

Sérülékeny kód

Hibás összefoglaló

Adatkezelési hiányosságok

Eltérő válasz ugyanarra a kérdésre

Szolgáltatófüggés

„A Sirius Kibernetikai Társaság valódi emberi személyiséggel ruházta fel a robotokat, ***és az eredmény egy örökké depressziós android lett.”****

Elutasítás

Tudatos, felelős, kockázatarányos MI-használat

Kontroll nélküli, könnyelmű használat

Arany középút

*: GALAXIS ÚTIKALAUZ Stopposoknak



Információbiztonság

Tudatos és felelős AI
fejlesztés és használat

Személyes adatok védelme

Az AI már nem (csak) IT-kérdés



Üzenet „Ha AI-t használunk, már szereplői vagyunk a történetnek.”

Információbiztonság
Sértetlenség, bizalmasság, rendelkezésre állás
NIS2 – ISO 27001

Tudatos és felelős AI használat
- Jártasság, dokumentáció
AI Act – ISO 42001

Személyes adatok védelme
Adatkezelés és -feldolgozás jogszerűen
GDPR

Szabályozás - ember a középpontban

AZ AI ACT CÉLJA (1. CIKK)

1. **Emberközpontú és megbízható MI elterjedésének előmozdítása**
2. Az egészség, a biztonság és az alapvető jogok magas szintű védelme a káros hatásokkal szemben
3. A belső piac működésének javítása és az innováció támogatása

AZ ELSŐ AI-SZABÁLYOK?

Asimov törvényei

1. Nem árthat az embernek, és nem hagyhatja, hogy baja essen.
2. Engedelmeskedik az embernek – ha ez nem sérti az 1. törvényt.
3. Védi önmagát – ha ez nem sérti az 1. és 2. törvényt.

Nulladik törvény: minden áron meg kell védenie az emberiséget

Üzenet **A technológia fejlődhet gyorsan. Az ember - és környezete - védelméről nem mondhatunk le.**

Nem minden AI egyformán kockázatos

Mire használjuk? → Kit érint? → Mi történhet, ha hibázik? → Mekkora a kockázat? → Mit kell tennünk?

A válasz kategóriát ad, és ahhoz igazodó kötelezettségeket:

Tiltott gyakorlatok
Elfogadhatatlan kockázat – nem alkalmazható

Nagy kockázat
Szigorú követelmények, életciklus-alapú kockázatkezelés (9. cikk)

Átláthatósági kötelezettség
Pl. jelezni kell, ha valaki MI-vel kommunikál

Egyéb, alacsony kockázat
Nincs külön előírás – a tudatos használat itt is számít

Mit jelent nekem? **Nem az eszköz dönt, hanem a felhasználás célja és hatása.**

MI-jártasság: A jogszabályi megfelelés az embereknél kezdődik

MI A MI-JÁRTASSÁG? (3. CIKK 56. PONT)

Készségek, ismeretek és értelmezési képesség, hogy tájékozottan használjuk az MI-rendszereket – és értsük lehetőségeiket, kockázataikat és lehetséges káraikat.

MIT VÁR EL A 4. CIKK?

Szolgáltatók és alkalmazók intézkedésekkel támogatják személyzetük és a nevükben eljárók MI-jártasságának fejlesztését.

FIGYELEMBE VÉVE:

- Szakmai ismeretek
- Tapasztalat
- Végzettség, képzettség
- A használat körülményei

KIT ÉRINT?

- Vezetők
- Munkatársak
- Nevünkben eljárók

Üzenet A tudatos MI-használat nem az IT-osztálynál kezdődik.

„Hogyan legyünk okosak?”

„A szuperszámítógép **7,5 millió év** alatt kiszámolta a végső választ:”

42 *

ISO/IEC 42001 – AI irányítási rendszer

Az MI-vel kapcsolatos teendőket szervezett működéssé alakítja:

- **Szerepek és felelősségek**
- **Kockázatkezelés**
- **Szabályzatok**
- **Kontrollok**
- **Kompetenciák**
- **Dokumentáció**

Monitorozás és folyamatos fejlesztés ↻

Fontos **Az ISO/IEC 42001 nem egyenlő az AI Act megfeleléssel, de jelentősen segíti a megfelelés tudatos, következetes működtetését.**

*: GALAXIS ÚTIKALAUZ Stopposoknak

Szabályból működés

AI Act

MIT és MIÉRT kell kezelnünk?

Kötelező uniós rendelet, kockázatalapú követelmények

+

ISO/IEC 42001

HOGYAN építsünk köré következetes működést?

Önkéntes nemzetközi szabvány, irányítási rendszer

MINDKETTŐ MÖGÖTT UGYANAZ A GONDOLATMENET

- Kockázat-alapúság
- Felelősségek
- Kompetencia
- Dokumentáltság
- Folyamatos kontroll

Nagy kockázatú rendszereknél az AI Act maga is előír kockázatkezelést (9. cikk), dokumentációt, emberi felügyeletet (14. cikk) és szervezeti követelményeket; a szabványok szerepét a 40. cikk rendezi.

Fontos

Két egymást kiegészítő keret, nem egyenlőségjel: a szabvány nem jelent automatikus megfelelést! Továbbá számos más szabvány, iránymutatás is elérhető

Mit jelent ez egy KKV-nak?

1

Felmérés

Hol használunk MI-t – hivatalosan vagy informálisan?

2

Felelősök kijelölése

Ki dönt az MI-eszközökről, és ki felügyeli őket?

3

Kockázatok értékelése

A konkrét felhasználási cél alapján.

4

Jártasság fejlesztése

Ne csak eszközhasználatot taníts, hanem gondolkodást is.

5

Dokumentálás, felülvizsgálat

Hogy a szervezet tanulni tudjon a használatból.

Nem egyedül!

Célzott képzések és tájékoztatás

Külön tanácsadói csatornák KKV-knak

Understand. Assess. Govern. Use.

„Az AI-tól nem félni kell. Meg kell tanulnunk felelősen bánni vele.”

„DON'T PANIC”