Kiberbiztonsági és információvédelmi technológiák innovációja

A Nemzeti Kiberbiztonsági Akcióterv 24. feladata

Varga Gábor
IVSZ – Digitális Vállalkozások Szövetsége · kiberbiztonsági munkacsoport vezetője

A kiberbiztonság fejlesztése innovációval



A stratégiai célok végrehajtási feladatokban testesülnek meg: a kiberbiztonsági innováció használatának ösztönzése.

White paper a szabályozási vonatkozásokról:
From Strategy to Implementation: National Cybersecurity Action Plan in Hungary
Varga, Gabor
DOI: 10.5281/zenodo.20555273
https://zenodo.org/records/20555273

CyberHubs

Nemzeti Kiberbiztonsági Akcióterv 24-es feladat

24 Szakmai fórum létrehozása a feltörekvő technológiák és felhőszolgáltatások kiberbiztonsági vizsgálatára

Fejezet	IV. Hazai szervezetrendszer megszilárdítása
Felelős	kiberbiztonságért felelős biztos
Közre-működők	NBSZ, felsőoktatási és kutatóintézmények, innovációs és kiberbiztonsági szervezetek, felhőszolgáltatók, hírközlési szolgáltatók, felhasználói szervezetek
Határidő	2026. november 30.

Leírás

Olyan szakmai fórumot kell létrehozni, amely folyamatosan vizsgálja a kiberbiztonság szempontjából releváns felhő- és egyéb feltörekvő technológiákat, eredményeiről rendszeresen tájékoztatja a kiberbiztonsági szabályozásban érintett szervezeteket.

A fórum koordinációjára célszerű felkérni egy technológiai iparágat reprezentáló szövetséget, például a Digitális Vállalkozások Szövetségét, vagy az alkalmazott tudományokkal foglalkozó kutatóintézetet, a HUN-REN SZTAKI-t.

A strukturális probléma

Szabályozó:
"az alanyok **akarják**-e használni"

Egymásra várás

Jogalanyok:
"a szabályozó **engedi**-e használni?"

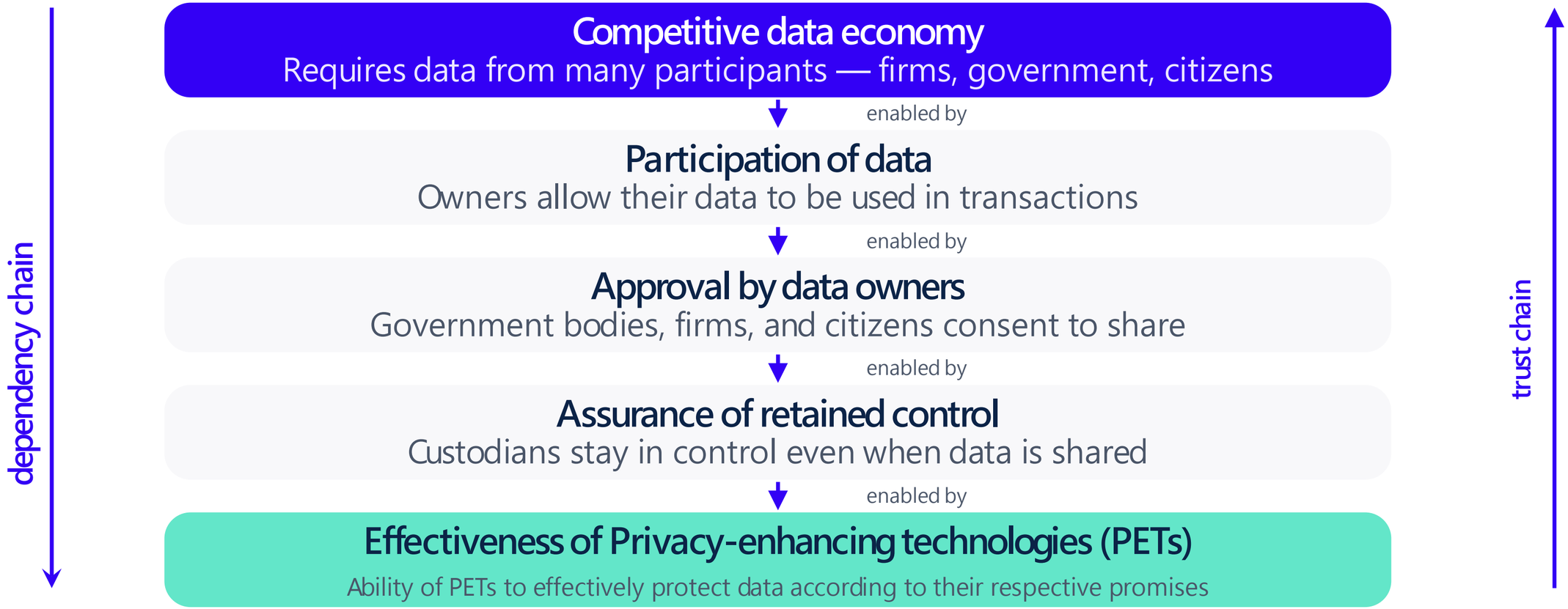
„Meg fognak-e bírságolni azért, ha x-y technológiát z módon használok?"

Jogalkotók és jogalanyok együttműködése szükséges.



CyberHubs

Adatgazdaság: bizalmi lánc és függőségi lánc



Prioritások a 24-es munkacsoport számára

Kiválasztási szempontok

1. fontos gazdasági vagy tudományos célok előtti akadályokat bontanak le
2. Magyarországon gazdátlanok, felkarolásra várnak
3. más szakmai fórumok még nem patronálják
4. nemzetközi szakmai közösségük már létezik, sikeres projektek vannak
5. nincs előttük jogszabályi akadály, legfeljebb annak percepciója

Olyan területek kapjanak figyelmet, ahol a szakmai közösség és a szabályozási bizalom együtt tud fejlődni.

CyberHubs

Az elsőként azonosított technológiák

Fókusz:	Alkalmazáskörnyezet (felhő)	Kvantumszámítás-technika	Tartalom és információ	Társadalom ellenállóképessége
Színtér:	Infrastruktúra	Infrastruktúra	Adat	Kognitív
Kockázat:	Felhő környezetek nem megbízhatók	Kvantumgépekkel a mai titkosítás feltörhető	Hagyományos titkosítás nem véd felhasználás közben	Deepfake-kel támogatott megtévesztés
Védelmi taktika:	Kriptográfiai bizonyíték a megbízhatóságra	Kvantumrezisztens kriptográfia	Álnevesítés modern módszerei	Médiafogyasztók támogatása a szintetikus média felismerésében
Technológiák és képességek:	**Confidential computing (bizalmi számítástechnika, CC):** • Titkosítás használat közben megbízható számítási környezetekben (TEE) **HSM:** biztonságos kulcskezelés **Sandbox**	**Post-quantum cryptography (PQC):** • Kvantumgépeknek ellenálló titkosítás adattovábbítás és tárolás közben	Privacy-enhancing technologies (PET), pl: **Differential privacy:** • Statisztikai zaj hozzáadása adatokhoz a személyek azonosítása ellen **Federált tanítás:** • Modellek tanítása a nyers adatok megosztása nélkül **Homomorf titkosítás:** • Számítások közvetlenül a titkosított adatokon **Egyéb releváns PET-ek**	**Származás igazolása:** • C2PA – Kriptográfiai módszerekkel alátámasztott származási lánc **Vízjelezés:** • SynthID – észlelhetetlen jelzések beágyazása létrehozáskor **Deepfake detektálása:** • Manipulált média felismerése AI segítségével **Jártasság:** • Felhasználói kritikus gondolkodás

Munkaterv a 24-es feladathoz

Előkészítés

2025. július 31

A Nemzeti Kiberbiztonsági Akcióterv megjelenése

1

2025. augusztus – 2026. március

SZTAKI, IVSZ;

KSH, NAIH

Alkalmazási lehetőségek feltárása

Kiemelt téma prioritások

Kiberfórum tájékoztatása

2

Megalakulás

2026. június 16.

Fórum megalapítása

3

Végrehajtás

2026. július – 2027. június

Műhelymunka

workshopok, kutatások, esettanulmányok stb.

4

Eredmények felajánlása gazdasági és kormányzati szereplők felé

5

CyberHubs

A mesterséges intelligenciával létrehozott tartalmak jelölése az AI Act szerint

… hogy visszakapjuk azt a világot, amelyben még hihettünk a szemünknek.

Varga Gábor • IVSZ – Digitális Vállalkozások Szövetsége
az információ- és kiberbiztonsági munkacsoport vezetője

2026. szeptember 2.

2026. augusztus 2-től alkalmazandó: az 50. cikk és jogi környezete

KÖTELEZŐ JOGFORRÁS

AI Act 50. cikk

Szolgáltatók + alkalmazók

Digital Omnibus módosítások

ÉRTELMEZÉS ÉS MEGFELELÉS

EC iránymutatás
Guidelines on transparency obligations for providers and deployers of AI systems

Átláthatósági Gyakorlati Kódex
Code of Practice on Transparency of AI-generated Content

Bizottsági vélemény + AI Board adequacy assessment

KAPCSOLÓDÓ JOG

Digital Services Act
(DSA 34. és 35. cikk)

2025. évi LXXV. törvény

344/2025. Korm. rendelet

+ a hamis közlést tiltó teljes joganyag

Az AI-jelölés nem váltja ki a büntetőjogi, polgári jogi, fogyasztóvédelmi, reklámjogi vagy platformszabályokat.

Az alkalmazó (deployer) a feladata a közlés:

DEEPFAKE

„deepfake”: az MI által generált vagy manipulált kép, audio- vagy videotartalom, amely hasonlít létező személyekre, tárgyakra, helyekre, entitásokra vagy eseményekre, és amely egy személy számára megtévesztő módon autentikusnak vagy valóságosnak tűnne;

→ Kivételek például:
Éneklő egerek,
Esztétikai módosítások,
Háttér lecserélése – amennyiben ezeknek nincs hatása a valóságként érzékelésre

→ További kivétel: bűnüldözési célból

KÖZÉRDEKŰ SZÖVEG

A nyilvánosságot közérdekű ügyben tájékoztató, AI-val létrehozott vagy manipulált szöveg.

→ Kivétel: megfelelő emberi felülvizsgálat vagy szerkesztési ellenőrzés (editorial control) és szerkesztői felelősség viselése.

A MI-rendszer alkalmazóját terhelő jelölés a „régi normalitáshoz” próbál visszatérni

AMI AZ AI KORSZAK ELŐTT NORMÁLIS VOLT: NEM KELL JELÖLNI

Érdemi átnézés.

Tények ellenőrzése.

Szerkesztői kontroll.

Nyilvánvaló fikció.

A mű értelmezését nem befolyásoló módosítás, pl. háttér lecserélése

Általában nem kell jelölni akkor sem, ha AI alkalmazásával jött létre.

AMI KORÁBBAN NEM VOLT NORMÁLIS: JELÖLNI KELL

Olvasatlan publikálás.
Valósnak tűnő, meg nem történt esemény képei.

Jelölni kell, ha AI alkalmazásával jött létre

Szemléltető összefoglalás, nem jogi tanács. A konkrét esetet az AI Act, a Guidelines és a Kódex alapján kell minősíteni.

Az eredetjelzés nem igazságpecsét, de nélkülözhetetlen támpont

A JELÖLÉS MEGMONDJA:

milyen szerepe volt az AI-nak a létrehozásban vagy a tartalommanipulációban

NEM MONDJA MEG:

hogy a közlés igaz, jogszerű, teljes vagy megbízható-e

A jelölés nem tesz mást, mint táplálja a kritikus gondolkodást.
A döntést a tartalomfogyasztó hozza a tartalomról. Dönthet úgy, hogy további elővigyázatossági lépéseket tesz: ellenőrzés, forráskeresés, óvatosság, továbbküldés megtagadása. Az AI Act ebben nem foglal állást, csak informál a jelöléssel.

ivsz
AI Kompetencia
Központ

Az Átláthatósági Gyakorlati Kódex könnyített út a megfeleléshez

✓ szolgáltatói jelölések (nem érzékelhető vízjel, érzékelhető metaadatok, detektáló eszköz)
✓ alkalmazói jelölések (deepfake, közérdekű ügyekről tájékoztató szöveg)
✓ következetes, arányos és interoperábilis gyakorlat
✓ dokumentált megfelelés
✓ részvétel a szabályozás továbbfejlesztésében

Az EU Bizottság és az AI Board megfelelő önkéntes eszköznek minősítette — de nem megfelelési bizonyíték.

Az IVSZ részt vett a Gyakorlati Kódex véleményezésében. A tagságtól érkező javaslatokat több körben továbbítottuk a Kódexet kidolgozó szakértőknek.

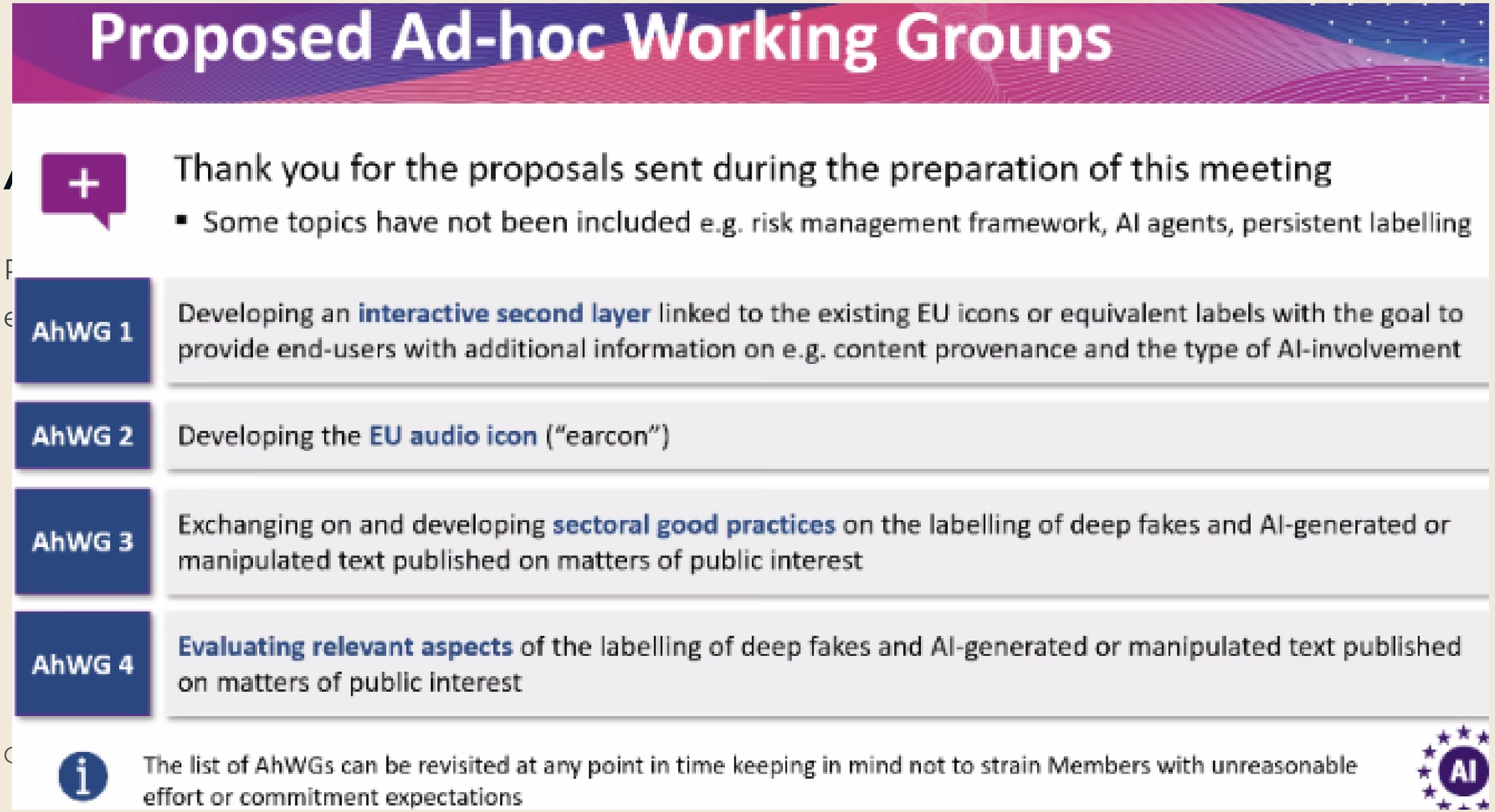
Eddigi legfontosabb lépéseink

01 **Részt vettünk az EU Adatvédelmi testület konzultációjában az anonimizálásról**
PET alkalmazási lehetőség.

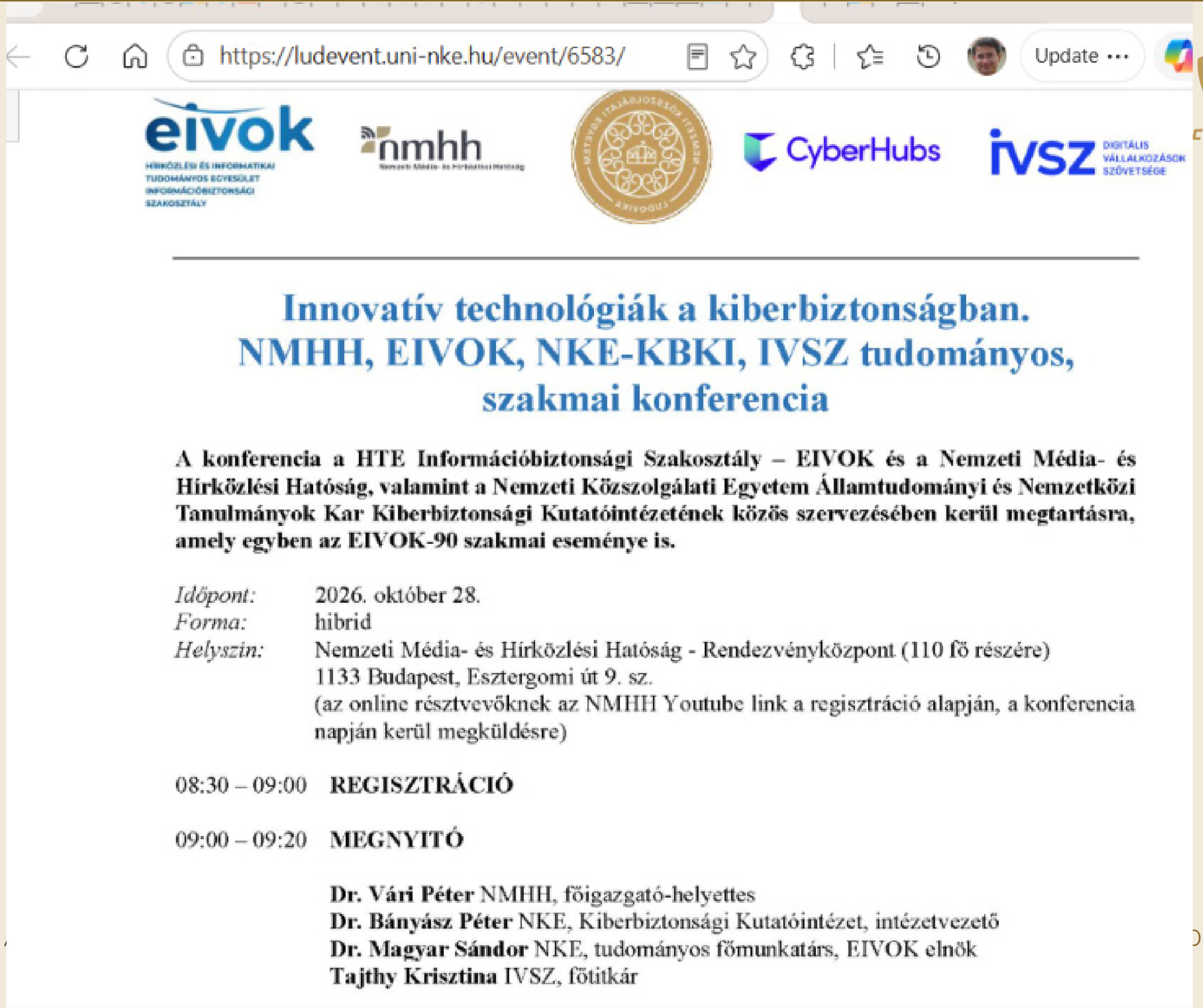
02 **A Mesterséges Intelligencia Piacfelügyelet tájékoztató webhelyet hozott lérte a jelölésekről**
véleményeztük és javaslatokat tettünk.

03 **Meghívást kaptunk és elkezdtük a munkát az Átláthatósági Gyakorlati Kódex fejlesztésével foglalkozó Task Force-ban**
Magyar javaslat is született.

Az AI Act Transparency Code of Practice Task Force
Deployers



Innovatív technológiák a kiber-biztonságban



https://ludevent.uni-nke.hu/event/6583/

Update

eivok
HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

nmhh

CyberHubs

ivsz DIGITÁLIS VÁLLALKOZÁSOK SZÖVETSÉGE

Innovatív technológiák a kiberbiztonságban. NMHH, EIVOK, NKE-KBKI, IVSZ tudományos, szakmai konferencia

A konferencia a HTE Információbiztonsági Szakosztály – EIVOK és a Nemzeti Média- és Hírközlési Hatóság, valamint a Nemzeti Közszolgálati Egyetem Államtudományi és Nemzetközi Tanulmányok Kar Kiberbiztonsági Kutatóintézetének közös szervezésében kerül megtartásra, amely egyben az EIVOK-90 szakmai eseménye is.

Időpont: 2026. október 28.
Forma: hibrid
Helyszín: Nemzeti Média- és Hírközlési Hatóság - Rendezvényközpont (110 fő részére)
1133 Budapest, Esztergomi út 9. sz.
(az online résztvevőknek az NMHH Youtube link a regisztráció alapján, a konferencia napján kerül megküldésre)

08:30 – 09:00 **REGISZTRÁCIÓ**

09:00 – 09:20 **MEGNYITÓ**

Dr. Vári Péter NMHH, főigazgató-helyettes
Dr. Bányász Péter NKE, Kiberbiztonsági Kutatóintézet, intézetvezető
Dr. Magyar Sándor NKE, tudományos főmunkatárs, EIVOK elnök
Tajthy Krisztina IVSZ, főtitkár

Köszönöm a figyelmet!

Varga Gábor
www.Linkedin.com/in/gaborvar