



**A NIS2 megfelelés humán
kockázati vonatkozásai, avagy
küldjünk e-magánnyomozót a
rendszergazdára?**

Dr. Szakolyi András

Tartalom, avagy a humán kockázat dilemmája

NIST SP 800-53
humán kockázati
gyakorlata

ISO/IEC 27001:2023
humán kockázati
gyakorlata

A hazai előírások

Jogi korlátok

Küldjük –e a
magánnyomzót?



NIST SP 800-53

<https://csf.tools/reference/nist-sp-800-53/r5/ps/>



PS: Personnel Security

- PS-1 Policy and Procedures (Szabályzat és Eljárásrendek)
- PS-2 Position Risk Designation (Pozíció Kockázati Besorolása)
- PS-3 Personnel Screening (Személyi Átvilágítás)
- PS-4 Personnel Termination (Munkaviszony Megszüntetése)
- PS-5 Personnel Transfer (Személyi Áthelyezés)
- PS-6 Access Agreements (Hozzáférési Megállapodások)
- PS-7 External Personnel Security (Külső Személlyzettel kapcsolatos biztonsági követelmények)
- PS-8 Personnel Sanctions (Személyi Szankciók)
- PS-9 Position Descriptions (Munkaköri Leírások)



NIST SP 800-53

Támogató kontrollok más családokból

- Awareness and Training (AT - Tudatosság és Képzés)
- Access Control (AC - Hozzáférés-szabályozás)
- Audit and Accountability (AU - Naplózás és Elszámoltathatóság)



<https://csf.tools/reference/nist-sp-800-53/r5/ps/>



ISO/IEC 27001:2022

<https://www.iso.org/standard/27001>



„A” Melléklet: Szervezeti, **Emberi**, Fizikai, Technológiai kontrollok

A 6. Kontroll család: Emberekkel kapcsolatos intézkedések

- 6.1 Szűrés (Screening)
- 6.2 Foglalkoztatási feltételek (Terms and conditions of employment)
- 6.3 Információbiztonsági tudatosság, oktatás és képzés (Information security awareness, education and training)
- 6.4 Fegyelmi eljárás (Disciplinary process)
- 6.5 Felelősségek a munkaviszony megszűnése vagy módosulása után (Responsibilities after termination or change of employment)
- 6.6 Titoktartási vagy nem nyilvánosságra hozatali megállapodások (Confidentiality or nondisclosure agreements)
- 6.7 Távmunkavégzés (*Remote working*)
- 6.8 Információbiztonsági események jelentése (Information security event reporting)



A hazai követelményrendszer

Kiberbiztonsági törvény

- Indirekt é direkt kötelezettségek

7/2024 (06.24) MK rendelet (126)

14. Személyi biztonság fejezet (38)

Támogató kontrollok más családokból

- 2. Hozzáférés-felügyelet: (32)
- 3. Tudatosság és képzés: (17)
- 4. Naplózás és elszámoltathatóság (12)
- 13. Készenléti tervezés: (4)
- 18. Rendszer- és információsértetlenség: 3)



7/2024 MK rendelet - 14. Személyi biztonság fejezet

14. Személyi biztonság fejezet

- 14.2. Munkakörök biztonsági szempontú besorolása
- 14.3. Személyek háttérellenőrzése
- 14.4. Személyek háttérellenőrzése – Különleges védelmi intézkedéseket igénylő információ (o)
- 14.5. Személyek munkaviszonyának megszűnése
- 4.6. Személyek munkaviszonyának megszűnése – Munkaviszony megszűnését követő követelmények (o)
- 14.7. Személyek munkaviszonyának megszűnése – Automatizált intézkedések (M)
- 14.8. Az áthelyezések, átirányítások és kirendelések kezelése
- 14.9. Hozzáférási megállapodások
- 14.10. Hozzáférási megállapodások – Munkaviszony megszűnése után is fennálló kötelezettségek (o)
- 14.11. Külső személyekhez kapcsolódó biztonsági követelmények
- 14.12. Fegyelmi intézkedések
- 14.13. Munkaköri leírások



A szabályozás logikája

1. Szervezeti keretek megteremtése

- Szabályozás
- Felelősségi körök

2. Munkavállalói életciklus

- Belépés
- Munkaviszony fennállása
- Munkaviszony megszűnése

3. Folyamatos kontroll

- Hozzáférés ellenőrzés
- Elszámoltathatóság
- Tudatosság
- Szankciók



Jogi korlátok: Munka Törvénykönyve

Mt. 11/A. §
"a munkáltató a
munkavállalót a
munkaviszonnyal
összefüggő
maga-tartása
körében
ellenőrizheti"

Csak a munkaviszonnyal összefüggő magatartás

Technikai eszköz csak tájékoztatással

A magánhasználat alapértelmezetten tilos

A magáncélú használat tilalmának ellenőrzését
alátámasztó adat kezelhető

Az emberi méltóság védelme - 9. § (2) bek



Jogi korlátok: Adatvédelem

Döntés száma	Ügy összefoglalása	Relevancia humán kockázat szempontjából
NAIH/2019/769	Munkáltató a távol lévő munkavállaló jelenléte nélküli átvizsgálta irodai asztalát, számítógépét és e-mail fiókját, majd megszüntette a munkaviszonyát.	Megerősíti a munkavállalói IT eszközök ellenőrzésének szigorú eljárásrendjét: előzetes szabályozás, jelenlét biztosítása, fokozatosság elvének betartása.
NAIH/2019/51/11	Volt munkavállaló archivált e-mail fiókjának tartalma és keresés azokban.	Rögzíti a kétszintű tájékoztatási kötelezettséget: általános és konkrét tájékoztatás szükséges.
NAIH/2019/2466/12	Munkáltató kamerarendszert üzemeltetett közösségi terekben tisztviselők állandó megfigyelésére.	Kimondja az állandó, cél nélküli kamerás megfigyelés tilalmát. Jogszerű cél igazolása szükséges.
NAIH/2022/903	Munkáltató folyamatos kontroll és totális megfigyeléssel tartotta a munkavállalókat kamerarendszerrel.	Megerősíti a folyamatos, totális megfigyelés tilalmát mint a tisztességes adatkezelés elvének sérelmét.
NAIH/2020/643/6	Munkavégzésre szolgáló helyiségekben és munkahelyiségben elhelyezett kamerák jogszerűségének vizsgálata.	Tisztázza a pihenőhelyiségekben történő kamerás megfigyelés tilalmát az emberi méltóság védelme érdekében.



Jogi korlátok: Adatvédelem

Döntés száma	Ügy összefoglalása	Relevancia humán kockázat szempontjából
NAIH/2019/1073	Irányútatás a hatósági erkölcsi bizonyítvány bekérésének és kezelésének feltételeiről.	Különleges adatok kezelése csak törvényi előírás esetén. Munkavállalói hozzájárulás nem érvényes jogalap.
NAIH Tájékoztató	Általános útmutató munkahelyi adatkezelésekről (kamera megfigyelés, GPS nyomkövetés).	GPS nyomkövetés korlátai: csak munkaidőben, munkavégzéssel összefüggésben, kikapcsolási lehetőséggel.
36/2005. AB határozat	Az Alkotmánybíróság általános elvi megállapítása: elektronikus megfigyelésről és magánszféráról.	Alapvető hivatkozási pont: elektronikus megfigyelés veszélyezteti a magánszférát és emberi méltóságot.
Bărbulescu kontra Románia	EJEB döntése a munkavállalói kommunikáció munkáltatói ellenőrzéséről.	Létrehozta a "Bărbulescu-tesztet" - több szempontú kritériumrendszer az ellenőrzés jogszerűségéhez.
WP 29. 2/2017	Európai Adatvédelmi Testület véleménye a munkahelyi adatkezelésről.	Hangsúlyozza az adatminimalizálást, célhoz kötöttséget és hatásvizsgálat szükségességét, jog a megfigyelésmentes internet kapcsolathoz.



Tanulságok és tipikus esetek

Adatvédelmi követelmények

- Jogalap
- Előzetes tájékoztatás
- Arányosság
- Célhoz kötöttség
- Szabályozás
- ÉMT/hatásvizsgálat
- „Barbulescu teszt”
- Munkaköri leírás
- Titoktartási nyilatkozat

Számítástechnikai eszköz egyedi ellenőrzése:
Előzetes tájékoztatás, jelenlét, magáncélú adatok esetén leállítás

IT magáncélú használat engedélyezése tiltása vagy speciális egyedi szabályozás alapján.

Erkölcsei bizonyítvány – csak a feltételek megléte esetén
(Az általános és a speciális tartalmat igazítsuk az alkalmazáshoz)

Kilépésnél nyilatkozat a magáncélú adatok törléséről a számítógépről és a levelezésből. Ezzel kapcsolatos jogi igények kizárása.

Internet használat ellenőrzése (DLP is) - teljesülnek – e a követelmények ?

Végzettségek ellenőrzése

Fiktív munkavállalók kiszűrése

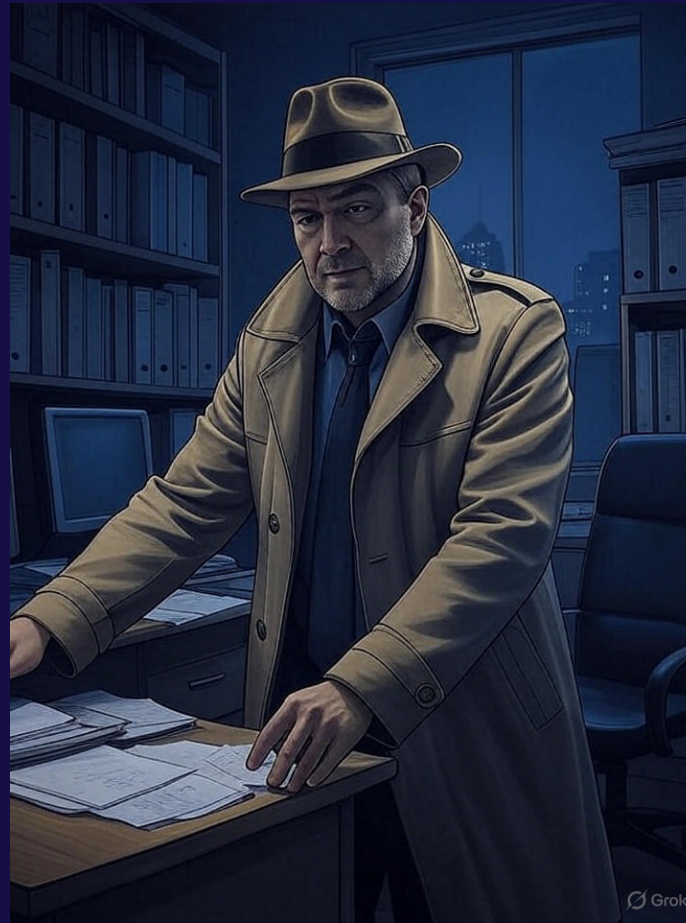


Hívjuk –e a magánnyomozót?

Feltételei:

- Előzetes (!) tájékoztatás
- Dokumentált, tényeken alapuló gyanú
- Más eszköz nincs

Példák: Bűncselekmény gyanúja,
üzleti titok megsértése [Mt. 8.§ (4)]



Köszönöm a figyelmet!

Szakolyi András

SBCS Consulting Kft.

szakolyi.andras@sbcs.hu

