A munkavállaló IT eszközeinek ellenőrzése - Iránymutatás

VFP2 KiberVéd - NIS2 Audit felkészítés szakmai iránymutatás 2026/2

VERZIÓKÖVETÉS

Verziószám	Dátum	Módosította	Módosítások leírása
1.0	2026.01.26	Kálmán és Társa Ügyvédi Iroda	Első kiadott verzió

1. ÖSSZEFOGLALÁS

A jelen dokumentum azt vizsgálja, milyen módon lehet a munkavállalót, a rendelkezésére bocsátott számítástechnikai eszközök megfelelő használatát jogszerűen ellenőrizni.

A Munka Törvénykönyve[1] szerint a munkavállaló a munkaviszonnyal összefüggő magatartása körében ellenőrizhető, ennek keretében a munkáltató technikai eszközt is alkalmazhat. A munkáltató az ellenőrzése során betekinthet azokba a munkaviszonnyal összefüggő adatokba, amelyeket a munkavállaló a munkaviszony teljesítéséhez használt számítástechnikai eszközön tárol (akár a munkáltató által biztosított, akár a munkavállaló saját eszközéről van szó).

A kiberbiztonsági szabályok (különösen a 7/2024. (VI. 24.) MK rendeletben (a továbbiakban: Rendelet) meghatározott követelmények) is lehetővé teszik a munkavállaló ellenőrzése (azaz esetleges szabályszegésének megállapítása) szempontjából lényeges adat gyűjtését (de az ellenőrzésnek nem kizárólag a kiberbiztonsági követelmények érvényesítése során történő adatgyűjtés az eszköze); ahhoz azonban, hogy ezeket az adatokat a munkavállalóval szemben fel lehessen használni, számos garanciális szabályt be kell tartani. E garanciális szabályokat részben a Munka Törvénykönyve, részben viszont a joggyakorlat alakította ki.

Adatvédelmi szempontból fontos rögzíteni, hogy bármilyen formájú/tartalmú is az adatkezelés, annak szabályszerűségéhez szükséges, hogy az adatkezelő (munkáltató) az adatkezelés megkezdése előtt a szükséges adatvédelmi dokumentumokat elkészítse. Ezek közé tartozik: az adatkezelési tevékenység nyilvántartása, az érintetteknek szóló adatkezelési tájékoztató, esetlegesen adatvédelmi hatásvizsgálat, illetve érdekmérlegelési teszt (ha az adatkezelés jogalapja az ún. jogos érdek).

Az ellenőrzéseket előzetesen kidolgozott szabályzat alapján kell lefolytatni. A Rendelet szerinti szabályzatok tartalmazhatnak erre vonatkozó rendelkezéseket, de nem fedik le teljes egészében a munkavállaló ellenőrzésének eljárásrendjét.

2. PROBLÉMAFELVETÉS

A NIS2 irányelv[2] hazai implementációját megvalósító Kiberbiztonsági tv.,[3] annak végrehajtási rendeletei, különösen a biztonsági osztályba sorolás követelményeiről valamint a Rendelet) megkövetelik, hogy a szervezetek az elektronikus információs rendszereiket (EIR) a kockázatokkal arányosan osztályozzák, és ehhez illeszkedően határozzák meg és valósítsák meg a védelmi intézkedéseket. A biztonsági osztályba sorolás alapján a szervezetnek meg kell

[1] a Munka Törvénykönyvéről szóló 2012. évi I. törvény (Mt.)

[2] Az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv) szóló, 2022. december 14-i (EU) 2022/2555 európai parlamenti és tanácsi irányelv

[3] A Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény

valósítania a rendeletben előírt védelmi intézkedéseket, és olyan kockázatmenedzsment keretrendszert kell működtetnie, amelynek keretében ezen védelmi intézkedések hatékonyságának folyamatos ellenőrzésére vonatkozó biztonságfelügyeleti stratégiát (módszereket, eszközöket és eljárásrendet) kell kidolgozni és végrehajtani. Jelen Iránymutatás szempontjából fontos kiemelni, hogy a Rendeletben meghatározott védelmi intézkedések számos ellenőrzési intézkedést is magukban foglalnak. A Kiberbiztonsági tv.-ben és a Rendeletben meghatározott követelmények érvényre juttatása tehát egyértelmű jogi kötelezettség, ami különböző jogkövetkezményekkel jár együtt.

E követelmények érvényre juttatása azonban csak az egyik lehetséges esetét és eszközét jelentik a munkavállaló ellenőrzésének és eszközeinek. A „munkavállaló ellenőrzése" számos más esetet is magába foglalhat. A Rendeletben meghatározott követelmények érvényesítése során gyűjtött adatok a kiberbiztonsági követelmények ellenőrzésén túl más típusú ellenőrzésekre is felhasználhatóak, feltéve, hogy a munkáltató megfelelő indokot tud felmutatni és igazolni.

A kérdés tehát az, hogyan egyeztethető össze a kiberbiztonsági követelmények érvényre juttatása során a munkáltatót megillető ellenőrzési jog (és részben kötelezettség) a munkavállalók jogaival.

3. INDOKOLÁS

3.1 A munkavállaló ellenőrzésének lehetősége

A Munka Törvénykönyve 11/A. §-a szerint:

a) csak a munkavállaló munkaviszonnyal összefüggő magatartása ellenőrizhető, magánélete nem;

b) az ellenőrzésnek számos módja lehet, ehhez a munkáltató technikai eszközt is igénybe vehet. Ebből következően lehetséges olyan ellenőrzés is, amelyhez a munkáltató nem vesz igénybe technikai eszközt (pl. a munkáltató képviselője a bejáratnál személyesen ellenőrzi, hogy mindenki időben érkezik-e). A technikai eszközzel történő ellenőrzés egyik lehetséges módja a munkáltató által a munkavégzéshez biztosított információtechnológiai vagy számítástechnikai eszközön, rendszerben (a továbbiakban: számítástechnikai eszköz) tárolt, a munkaviszonnyal összefüggő adatokba történő betekintés. Egyéb eszközök lehetnek pl. a munkáltató egyéb számítástechnikai eszközein (pl. szerverein) és rendszereiben tárolt adatok felhasználása, kamerás megfigyelőrendszerek működtetése, aktivitásmérők telepítése a munkavállaló által használt eszközökre, különböző beléptetőrendszerek, GPS navigációs rendszerek, testkamera használatának előírása, biometrikus rendszerek alkalmazásával folytatott ellenőrzés, a munkaidő nyilvántartására alkalmas rendszerek működtetése stb. Ezek nem mindegyike esik az elektronikus információs rendszereik (EIR) körébe, de mindegyik megfelel(het) az igénybe vehető „technikai eszköz" fogalmának;

c) minimális garanciális követelményként az Mt. előírja, hogy a technikai eszközzel történő ellenőrzésről munkavállalót előzetesen írásban tájékoztatni kell. Más típusú ellenőrzés esetén ilyen követelményt az Mt. nem támaszt (ez azonban nem érinti az adatvédelmi

jogszabályok szerinti tájékoztatási kötelezettséget, amely minden adatkezelésre egyaránt vonatkozik);

d) az Mt. továbbá tisztázza azt is, hogy a munkáltató azon adatokat is jogszerűen felhasználhatja az ellenőrzés során, amely adatok ahhoz kellenek, hogy a munkáltató által a munkavégzéshez biztosított számítástechnikai eszköz kizárólag munkavégzés céljából történő használatát ellenőrizhesse. Nem kizárt tehát, hogy bizonyos, egyébként nem a munkaviszonnyal összefüggő (tehát magántermészetű) adatok is kezelhetőek az ellenőrzés során.

3.2 Az ellenőrzési tevékenység, mint adatkezelés

A munkavállaló tevékenységének ellenőrzése szükségképpen adatkezeléssel jár, hiszen a munkavállalókra, mint természetes személyekre vonatkozó információk gyűjtése, tárolása, elemzése, rendszerezése stb. történik. Ez minden jellegű ellenőrzésre vonatkozik.

Az ellenőrzés fajtáját az Mt. nem határozza meg, az lehet folyamatos (pl. az EIR folyamatos monitorozása és az annak alapján szükséges intézkedések megtétele), de lehet *ad hoc* ellenőrzés akár egy konkrét gyanú felmerülése esetén, akár „szúrópróbaszerűen".

A szervezetnek tehát ***számba kell vennie, milyen típusú ellenőrzéseket kíván alkalmazni***. Ezek közé tartozik a Rendeletben meghatározott (kiberbiztonsági) követelmények érvényre juttatásának ellenőrzése is (a Rendelet számos ellenőrzési kötelezettséget is tartalmaz), és ezen ellenőrzéseket a szervezet köteles is elvégezni. Ezek sokszor automatikus intézkedésekben nyilvánulnak meg (pl. felhasználó fiókjának zárolása meghatározott számú sikertelen bejelentkezési kísérlet után), sem a felhasználók, sem a munkáltatók nem érzik ellenőrzésnek. A Rendelet tartalmaz azonban olyan ellenőrzéseket is (pl. az opcionális *4.44. Információk kiszivárgásának figyelemmel kísérése* vagy Magas biztonsági osztály esetében előírt *6.39. Rendszerelem leltár – Jogosulatlan elemek automatikus észlelése*), amelyek után a munkáltató – a szükséges kiberbiztonsági intézkedéseken felül – jogi lépéseket is tehet a munkavállalóval szemben.

A Rendeletben meghatározott követelmények érvényesítése során gyűjtött adatok azonban más típusú ellenőrzésekre is felhasználhatóak. A munkavégzéshez használt számítástechnikai eszközök be- és kikapcsolásának ideje, a munkaállomás zárolásának logolása támpontot adhat ahhoz, hogy a munkavállaló dolgozott-e egy adott időpontban vagy sem (miközben önmagában ezek az információk nem utalnak kiberbiztonsági veszélyre). A Covid-járvány óta elterjedt pl. a home office lehetősége, azaz a munkavállaló otthonából történő munkavégzés.

Ezzel kapcsolatban a Rendelet 2. számú melléklete már Alap biztonsági osztályban előírja 2.100 pontban, hogy a szervezett dolgozza ki és dokumentálja az engedélyezett távoli hozzáférés minden egyes típusára vonatkozóan a használati korlátozásokat, a konfigurációs vagy csatlakozási követelményeket és az alkalmazási útmutatókat, továbbá folytasson le előzetes engedélyezési eljárást a rendszerhez való távoli hozzáférés minden egyes típusára.

Amennyiben a munkáltató a home office lehetőségét akként biztosítja, hogy a munkavállalónak egy bizonyos időtartamon (pl. két órán) belül képesnek kell lennie a munkahelyére való beérkezésre, a munkavállaló által használt számítástechnikai eszköz IP címének rögzítése alkalmas lehet annak ellenőrzésére is, hogy a munkavállaló betartotta-e ezt a szabályt (és nem pl. egy tengerparti nyaralóhelyről „dolgozik"). Hasonlóképpen, ha pl. a munkavállaló azért kap bérkiegészítést, mert a munkáltató székhelye szerinti országban kell dolgoznia („expat"), az IP cím alapján történő helymeghatározás alkalmas lehet annak ellenőrzésére, hogy a munkavállaló egy bizonyos időszakban jogosult volt-e a bérkiegészítésre (azaz a home office-t nem egy egzotikus helyen alakította-e ki messze távol a munkáltató székhelyétől).

Általánosságban is kijelenthető, hogy a Rendeletben meghatározott követelmények érvényesítése során gyűjtött adatok nem csak a kiberbiztonsági követelmények érvényre juttatása céljából használhatóak fel, hanem más célra is, pl. a munkavégzéshez kapcsolódó jogi követelmények betartásának ellenőrzésére is. Ez utóbbi esetben (tehát a két említett példában és az ahhoz hasonló esetekben) azonban az említett adatok felhasználása már nem a kiberbiztonság érvényre juttatása érdekében történik, azaz adatkezelés célja más, mint amit a Kiberbiztonsági tv. vagy a Rendelet meghatároz.[4] Míg a Rendeletben meghatározott kiberbiztonsági követelmények érvényre juttatása terén legfeljebb a feltárt jogsértések (munkajogi, polgári jogi vagy büntetőjogi) következményeinek meghatározása során mérlegelhet a munkáltató, addig az ilyen addicionális ellenőrzéseknek már a lehetőségét is külön igazolnia kell a munkáltatónak (adatvédelmi szempontból: igazolnia kell, hogy jogos érdeke áll fenn az ellenőrzés lefolytatásához).

Bármilyen formájú is az adatkezelés, annak szabályszerűségéhez szükséges, hogy az adatkezelő (munkáltató) az adatkezelés megkezdése előtt a szükséges adatvédelmi dokumentumokat elkészítse. Ezek közé tartozik: az adatkezelési tevékenység nyilvántartása, az érintetteknek szóló adatkezelési tájékoztató, esetlegesen adatvédelmi hatásvizsgálat, illetve érdekmérlegelési teszt (ha az adatkezelés jogalapja az ún. jogos érdek).

Itt érdemes kitérni a kiberbiztonsági szabályok jogi minőségére a GDPR[5] jogalapjai szempontjából. A GDPR szerint az adatkezelés jogszerű, ha az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges. Ez két dolgot jelent: legyen egy olyan jogszabályi előírás, ami az adott szervezetre vonatkozik és ami alól nem tudja kivonni magát, illetve, hogy ez a jogi kötelezettség szükségessé tegye személyes adatok kezelését, azaz a jogi kötelezettség nem teljesíthető anélkül, hogy személyes adatok kezelésére ne kerülne sor.

A GDPR 32. cikke szerint az adatkezelő *„a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre annak érdekében,*

[4] Lsd. pl. a Kiberbiztonsági tv. preambulumbekezdései

[5] a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről szóló, 2016. április 27-i, (EU) 2016/679 európai parlamenti és tanácsi rendelet (általános adatvédelmi rendelet)

hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja". Nem nehéz ezt a rendelkezést párhuzamba állítani a kiberbiztonsági szabályok kockázatarányos védelem elvét megfogalmazó rendelkezéseivel,[6] effektíve ugyanarról van szó: az adott jogszabály hatálya alá tartozó szervezet[7] köteles meghatározott adatbiztonsági követelményeket érvényesíteni, ennek elmulasztása pedig jogkövetkezménnyel jár (azaz az adott szervezet nem tudja kivonni magát a követelmények érvényre juttatása alól). Másként fogalmazva: a NIS2 irányelven alapuló Kiberbiztonsági tv., illetve a Rendelet a GDPR 32. cikkében írt adatbiztonsági követelmények részletes kifejtését tartalmazza.

A Rendeletben meghatározott követelmények számos esetben utalnak ellenőrzésre, ellenőrzési kötelezettségre.[8] Ezek az ellenőrzési kötelezettségek tehát ugyanúgy jogi kötelezettségek, mint az egyéb kiberbiztonsági követelmények érvényre juttatása. Az ellenőrzés szerves részét képezi a kiberbiztonsági követelményeknek, azok érvényre juttatásának, tehát a Rendeletben meghatározott követelmények ellenőrzése során történő adatkezelés akkor is jogi kötelezettség, ha a Rendelet külön nem említi.[9]

3.3 A Rendeletben meghatározott követelmények, mint adatkezelési műveletek

Adatkezelési műveletek azok a műveletek, amelyeket személyes adatokon végeznek. A Rendeletben meghatározott követelményeknek nem mindegyikének érvényre juttatása jár személyes adat kezelésével (pl. egy szabályzat kidolgozása nem adatkezelési művelet, de egy naplózási művelet már igen).

A szervezetek előtt kettős feladat áll:

a) meghatározni, hogy mely követelmények járnak (járhatnak) személyes adatok kezelésével,[10]
b) ezen belül, milyen egyéb, fentebb említett – nem kiberbiztonsági követelmények, hanem a munkavégzés szabályszerűségének ellenőrzésére hivatott – estekben kívánja a munkáltató az adatokat felhasználni;
c) meghatározni, hogy milyen személyes adatok kezelésére van feltétlenül szükség a követelmény érvényre juttatásához.

---

[6] Lsd. pl. a „zárt, teljes körű, folytonos és a kockázatokkal arányos védelem" törvényi definícióját, Kiberbiztonsági tv. 4. § 99. pont

[7] Jelen esetben eltekinthetünk a GDPR és a Kiberbiztonsági tv. személyi hatálya közti különbségektől, az utóbbi alá tartozó szervezetek túlnyomó többsége a GDPR hatálya alá is tartozik; a két jogszabály tárgyi hatálya közti különbség pedig akkor lenne releváns, ha a Kiberbiztonsági tv. hatálya alá tartozó szervezetek nem kezelnének semmilyen személyes adatot, ami megint csak nem jellemző.

[8] Lsd. pl. 2.17. Hozzáférési szabályok érvényesítése – Kötelező hozzáférés-ellenőrzés; 2.20. Hozzáférési szabályok érvényesítése – Szerepkör alapú hozzáférés-ellenőrzés; 2.26. Hozzáférési szabályok érvényesítése – Tulajdonság alapú hozzáférés-ellenőrzés; 2.52. Információáramlási szabályok érvényesítése – Szűrési műveletek ellenőrzése; stb.

[9] A Rendelet számos esetben nem is ellenőrzésnek nevez egy-egy követelményt, hanem „figyelemmel kísérésnek", „nyomon követésnek" stb.

[10] E körben nyomatékosan hangsúlyozni kell, hogy személyes adatnak minősül minden olyan információ, amely egy azonosított vagy azonosítható természetes személyre vonatkozik. Ez a definíció jóval szélesebb, mint az alapvető személyazonosító adatok köre (a személyes adatok köre nem korlátozódik azokra az információkra, amely egy természetes személyt azonosít).

Például a *„2.71. Sikertelen bejelentkezési kísérletek”* követelmény érvényre juttatása személyes adat kezelésével jár (mivel egy adott felhasználó sikertelen bejelentkezésére vonatkozik), és legalább a felhasználó azonosító adatai, a sikertelen kísérletek száma, az egyes sikertelen bejelentkezési kísérletek ideje, a zárolás ténye, és a rendszergazda értesítésének ténye és ideje minősülhet szükséges személyes adatnak. Itt érdemes arra is utalni, hogy ha az adatkezelési művelet naplózásból áll, a naplózás nem feltétlenül egyes követelmények szerint elkülönítve történik, illetve történhet, tehát a napló tartalma számos követelmény érvényre juttatásához szükséges adatot tartalmaz(hat).

A különböző szabályzatok „megismertetése” is szükségessé *teheti* személyes adatok kezelését, de ez nagyban függ a megismertetés konkrét módjától: intraneten történő közzététel nem teszi szükségessé személyes adat kezelését, de egy minden érintettől elvárt nyilatkozat kitöltésében álló megismertetés már személyes adat kezelését eredményezi (pl. a nyilatkozó azonosító adata, a nyilatkozat ténye, a nyilatkozat ideje). Ez utóbbi akkor lehet indokolt – esetleges jogszabályi előírásokon túli esetekben – ha a szabályzat jelentősége azt indokolja.

A fentebb vázolt feladatok elvégzése során – adatvédelmi szempontból nézve – a célhoz kötöttség és az adattakarékosság elveinek [GDPR 5. cikk (1) bek. b) és c) pont] érvényre juttatása történik.

3.4 A munkavállaló ellenőrzésére vonatkozó releváns joggyakorlat

3.4.1 Az Európai Adatvédelmi Testület (EDPB) állásfoglalásai

Az Európai Adatvédelmi Testület elődje, a 29. cikk szerinti Adatvédelmi Munkacsoportnak (továbbiakban: WP29) a GDPR szabályait is figyelembe vevő 2/2017. számú, a munkahelyi adatkezelésről szóló véleménye[11] az internet használat megfigyelésével kapcsolatban megállapítja, hogy *„Helyes gyakorlat, ha a munkáltató másik hozzáférést is biztosít a munkavállalóknak, amely nem áll megfigyelés alatt. Ez megvalósítható ingyenes vezeték nélküli internet-hozzáférés vagy különálló készülékek/terminálok biztosításával (a közlések bizalmasság biztosító, megfelelő óvintézkedések mellett), amelyeken a munkavállalók gyakorolhatják a munkahelyi eszközök bizonyos mértékű magáncélú használatához való törvényes jogukat. A munkáltatónak emellett figyelemmel kell lennie arra, hogy bizonyos típusú forgalmak — mint például a magáncélú webes levelezés, az online banki funkciók használata vagy az egészségügyi honlapok felkeresése — elfogása veszélyeztetheti a munkáltató jogos érdekei és a munkavállalók magánélethez való joga közötti megfelelő egyensúlyt.”* – Ez a cél elérhető úgy is, ha a munkavállaló kikapcsolhatja a megfigyelésre szolgáló rendszert.

A WP29 a belső szabályozás fontosságát és a hatásvizsgálat elvégzésének szükségességét is hangsúlyozza:

„…Ki kell dolgozni egy szabályzatot arra, hogy mikor és ki férhet hozzá a gyanús naplózási adatokhoz, és ezt folyamatosan elérhetővé kell tenni valamennyi munkavállaló számára…”

„…Helyes gyakorlat, ha ennek felmérésére egy adatvédelmi hatásvizsgálat keretében kerül sor, még mielőtt bármilyen megfigyelési technológia bevezetésre kerül. Emellett a munkáltatóknak az

[11] https://www.naih.hu/files/wp249_hu_munkahelyi_adatkezelesek.pdf

adatvédelmi szabályzat mellett az elfogadható használatra vonatkozó szabályzatot is be kell vezetniük és közzé kell tenniük, amelyben meghatározzák a szervezet hálózatának és berendezéseinek megengedett használatát, és részletesen ismertetik az alkalmazott adatkezelést."

„A munkavállalók számára érdemi tájékoztatást kell nyújtani az alkalmazott számára a megfigyelésről, annak céljáról és körülményeiről, valamint arról, hogy a munkavállalóknak milyen lehetőségük van az adataik megfigyelési technológiák alóli kivonására. A jogszerű megfigyelésre vonatkozó politikáknak és szabályoknak egyértelműeknek és könnyen elérhetőeknek kell lenniük."

A BYOD (saját eszköz munkacélú használata) ellenőrizhetősége kapcsán az Adatvédelmi Munkacsoport megfogalmazta, hogy:

„A magánjellegű információk megfigyelésének elkerülése érdekében megfelelő intézkedésekkel kell különbséget tenni az eszköz magán- és munkacélú használata között."

„Másfelől a munkáltatónak azt is meg kell fontolnia, hogy szükséges-e adott munkacélú eszközök magáncélú használatát megtiltani, ha nincs mód a magáncélú használat megfigyelésére – például abban az esetben, ha az eszköz távoli hozzáférést biztosít olyan személyes adatokhoz, amelyek adatkezelője a munkáltató."

A WP29 a célhoz kötöttség elvére is emlékeztet, miszerint

„A munkavállalók pontos belépési és kilépési idejének, illetve a belépések gyakoriságának folyamatos megfigyelése azonban nem lehet indokolt, amennyiben azt más célra, például a munkavállalók teljesítményének értékelésére is használják."

A GPS nyomkövetők használatával kapcsolatos példán keresztül az Adatvédelmi Munkacsoport az adatminimalizálás szükségességét is hangsúlyozta:

„A folyamatos megfigyelésből származó adatok rögzítését és a munkáltató számára elérhetővé tett információkat a lehető legkisebb mértékűre kell csökkenteni. A munkavállalók számára lehetővé kell tenni, hogy ha ezt a körülmények indokolják, ideiglenes kiiktathassák a tartózkodási hely nyomon követését."

„Az új technológiák alkalmazására vonatkozó döntéseknél a munkáltatóknak figyelembe kell venniük az adatminimalizálás elvét. Az adatok csak a minimálisan szükséges ideig tárolhatók, az adatmegőrzési idő meghatározása mellett. Amint valamely adatra már nincs szükség, azt törölni kell."

3.4.2 Nemzetközi gyakorlat

Keylogger alkalmazásának tilalma Németországban: A német Szövetségi Munkaügyi Bíróság (Bundesarbeitsgericht) GDPR előtti döntése[12] értelmében keylogger szoftver használatával szerzett bizonyítékok felhasználása az adatvédelmi törvények szerint nem megengedett, ha nem merül fel bűncselekmény gyanúja. Az ilyen ellenőrzés csak akkor megengedett, ha a munkáltatónak konkrét gyanúja van a munkavállaló által elkövetett bűncselekménynek vagy

[12] Lsd. az esetismertetést a **https://www.dataprotectionreport.com/2017/08/german-court-monitoring-of-employees-by-key-logger-is-not-allowed/** oldalon

bármely más súlyos kötelességszegésnek egy konkrét esetben. Vagyis a felhasználás célja nem lehet általános, csak konkrét, körülhatárolt esetekben lehetséges ilyen megfigyelési technikát alkalmazni. Noha a döntés a GDPR előtti és a német munkajogi szabályokon is alapul,[13] de a hivatkozott döntés elvi alapjai miatt Magyarországon sem kizárt ilyen hatósági értelmezés.

Dolgozók teljes körű megfigyelése Olaszországban: Bolzano város önkormányzata megfigyelte a dolgozói számítógépes tevékenységét, de elmaradt a hatásvizsgálat és munkavállalók tájékoztatása, továbbá aránytalannak találta a hatóság a megfigyelést. Az olasz adatvédelmi hatóság (Garante) 84.000 EUR büntetést szabott ki és többek között kimondta, hogy még a munkáltató által biztosított hálózaton sem valósítható meg az internet használat teljes körű megfigyelése.

3.4.3 A „Bărbulescu-teszt”

A kérdéses ügyben a munkáltató folyamatosan monitorozta a munkavállalók kommunikációját a vállalati eszközökön, és tiltotta a vállalati eszközök magáncélú használatát. Az Emberi Jogok Európai Bíróságának Bărbulescu-ítélete[14] az alábbi kritériumokat támasztotta a munkavállaló ellenőrzésének jogszerűsége kérdésében:

- Előzetesen és világosan tájékoztatták-e a munkavállalót az ellenőrzés lehetőségéről és annak módjáról?
- Milyen jellegű és mértékű az ellenőrzés? Az kiterjed-e a konkrét tartalom megfigyelésére, vagy csak adatforgalmi mennyiségi adatokat érint? Minden kommunikációt ellenőriznek, vagy csak bizonyos formáit? Meddig tart az ellenőrzés és annak eredményeit ki jogosult megismerni?
- Mi indokolja a munkáltató a magánszférát korlátozó megfigyelés szükségességét? Ez megfelelő indok-e?
- Az adott eset kapcsán lett volna a munkavállaló magánszféráját kevésbe korlátozó olyan ellenőrzés, mellyel a kívánt cél szintén elérhető lett volna?
- Mik a megfigyelés következményei a munkavállalóra nézve? Ezek arányosak-e az elérni kívánt céllal?
- Az ellenőrzés belső rendje tartalmaz-e megfelelő biztosítékokat – pl. előzetes figyelmeztetés, jogorvoslat – a munkavállaló tevékenységének ellenőrzése kapcsán?

Ez a fenti teszt hasznos lehet a munkáltató számára annak felmérése során, hogy megfelelően alakította-e ki a munkahelyi ellenőrzéssel kapcsolatos gyakorlatát, melyet célszerű a hatásvizsgálat keretében elvégezni. Meg kell azonban jegyezni, hogy a Rendeletben meghatározott követelmények érvényesítése – ahogy fentebb kifejtésre került – jogi kötelezettség, tehát a magánszférába való beavatkozás indokoltságát a jogszabály adja meg. A beavatkozás konkrét mértékének meghatározásakor azonban a fenti teszt mindenképpen alkalmazható és alkalmazandó.

---

[13] A munkajogi adatkezelési szabályok tekintetében a GDPR jelentős szabadságot ad a tagállamok számára, így jelentős eltérések is lehetnek a tagállami szabályok között, vö. GDPR 88. cikk.

[14] Emberi Jogok Európai Bírósága Bogdan Mihai Barbulescu kontra Románia ítélete (61496/08.)

3.4.4 A López Ribalda-ügy

Az Emberi Jogok Európai Bírósága előtti López Ribalda vs. Spanyolország ügyben[15] az alapul fekvő tényállás szerint egy szupermarket vezetése az árukészleteiben hosszabb időn keresztül jelentős hiányt tapasztalt. Arra gyanakodva, hogy a dolgozók károsítják meg a vállalatot, a vezetőség látható és rejtett kamerákat szerelt föl, amikről a dolgozókat azonban (a spanyol jog előírása ellenére) nem tájékoztatták. Tíz napon belül a felvételek segítségével azonosítottak és azonnali hatállyal elbocsátottak egy tucatnyi dolgozót. A Bíróság előtt a kérelmezők a személyiségi jogaik (köztük a magánélet védelméhez való jog) megsértésére hivatkozott. A Bíróság azonban az eset összes körülményeire, így különösen a régóta tartó, szervezett és súlyos jogsértés gyanújára, illetve a pénztár környékére szorítkozó és időben is korlátos megfigyelésre tekintettel nem állapította meg az Emberi Jogok Európai Egyezményének a megsértését. Ez az eset azonban inkább a kivétel, mint a főszabály.

3.4.5 A Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) állásfoglalásai

A magyar adatvédelmi hatóság, a NAIH is kibocsátott számos határozatot, illetve tájékoztatót[16] a munkavállalók megfigyelése témakörében. A legrelevánsabbak lényegi összefoglalóját az alábbi táblázat tartalmazza:

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.

[15] Emberi Jogok Európai Bírósága López Ribalda és társai kontra Spanyolország ítélete (***1874/13*** *és* ***8567/13***)

[16] A Nemzeti Adatvédelmi és Információszabadság Hatóság tájékoztatója a munkahelyi adatkezelések alapvető követelményeiről
https://naih.hu/files/2016_11_15_Tajekoztato_munkahelyi_adatkezelesek.pdf

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.
NAIH/2019/1073	Iránymutatás a hatósági erkölcsi bizonyítvány bekérésének és kezelésének feltételeiről.	Különleges adatok kezelése csak törvényi előírás esetén lehetséges. Munkavállalói hozzájárulás nem érvényes jogalap.
36/2005. AB határozat	Az Alkotmánybíróság általános elvi megállapítása: elektronikus megfigyelésről és magánszféráról.	Alapvető hivatkozási pont: elektronikus megfigyelés veszélyezteti a magánszférát és emberi méltóságot.

A NAIH több döntésében is kiemelte az előzetes tájékoztatás szükségességét. A NAIH/2019/769 határozat[17] szerint *„a tisztességes adatkezelés elve megköveteli, hogy az érintett tájékoztatást kapjon az adatkezelés tényéről és céljairól, továbbá minden olyan információról, amelyek a tisztességes és átlátható adatkezelés biztosításához szükségesek."* A NAIH/2019/2466/ határozat szerint pedig *„az adatkezelés esetében lényeges követelmény, hogy az érintett az adatkezelésről megfelelő, átlátható és könnyen értelmezhető tájékoztatást kapjon."*

A NAIH/2019/51/11 határozat részletesebben is megfogalmazta a tájékoztatással kapcsolatos követelményeket. A tájékoztatásban a munkáltatónak ki kell térnie a GDPR 13. cikk (1)-(2) bekezdés szerinti adatkezelési körülményeire, azok közül kiemelt figyelmet fordítva arra, hogy:

- milyen célból, milyen munkáltatói érdekek miatt kerülhet sor (például) az e-mail-fiók áttekintésére (GDPR 13. cikk (1) bekezdés c) és d) pont),
- a munkáltató részéről ki, milyen módon végezheti az áttekintést (GDPR 13. cikk (1) bekezdés a) pont, mint az adatkezelő nevében az áttekintést folytató képviselője),
- milyen szabályok szerint kerülhet sor az adatkezelésre (fokozatosság elvének betartása) és mi az eljárás menete (GDPR 13. cikk (1) bekezdés c) pont),
- milyen jogai és jogorvoslati lehetőségei vannak a munkavállalónak az adatkezeléssel kapcsolatban (GDPR 13. cikk (2) bekezdés b) és d) pont).

Az általános tájékoztatáson túlmenően lehetőleg a konkrét intézkedés előtt is tájékoztatni kell a munkavállalót arról, hogy milyen munkáltatói érdek miatt kerülhet sor az adatkezelésre.

Ami az ellenőrzés lefolytatását illeti, a NAIH/2019/769 határozata kimondta, hogy a tisztességes adatkezelés elvéből egy olyan követelmény is származik, hogy az ellenőrzés során főszabályként biztosítani kell a munkavállaló jelenlétét. Az adatkezelés tisztességes volta a jogszerűséget is magában foglaló követelmény, az érintett információs önrendelkezési jogának, és ezen keresztül magánszférájának, emberi méltóságának tiszteletben tartását jelenti: az érintett nem válhat kiszolgáltatottá az adatkezelővel, sem más személlyel szemben. Az adatalany mindvégig alanya

[17] naih.hu/files/NAIH-2019-769-hatarozat.pdf

kell, hogy maradjon a személyes adatok kezelésével járó folyamatnak, és nem válhat annak puszta tárgyává. A munkavállaló jelenléte nélküli ellenőrzés ezért alapvetően ellentétes a tisztességes adatkezelés elvével. A NAIH egyes rendkívüli esetekben ezért elfogadhatónak tartja azt is, ha a munkavállaló nincs jelen, például azonnali intézkedést igénylő esetekben vagy betegállományban lévő munkavállaló esetében sürgős intézkedési szükség esetén. Ebben az esetben is azonban egyrészt tájékoztatást kell nyújtani a munkavállaló számára a tervezett munkáltatói intézkedésről, másrészt lehetőséget kell biztosítani számára arra is, hogy ha ő nem is tud jelen lenni, helyette meghatalmazottja vagy képviselője legyen jelen az ellenőrzésnél. Amennyiben ezen megelőző intézkedések – előzetes tájékoztatás és a munkavállaló vagy meghatalmazottja, képviselője jelenlétének biztosítása – ellenére a munkavállaló nem érhető el vagy nem jelenik meg sem személyesen, sem képviselője útján, akkor távollétében, független harmadik személy alkalmazásával is hozzá lehet férni az e-mailfiókjához, számítástechnikai eszközeihez az ellenőrzés, illetve az azonnali intézkedések végrehajtása érdekében. Ilyen esetben is meg kell ugyanakkor mindent tenni annak érdekében, hogy az ellenőrzés körülményei olyan módon legyenek rögzítve (adott esetben az ellenőrzés eredményében nem érdekelt személyek mint hitelesítő személyek jelenléte mellett vagy más megfelelő módon), hogy annak pontos menete, az annak során megismert adatok köre, azaz a ténylegesen elvégzett adatkezelési műveletek, és azok jogszerűsége utólag ellenőrizhető legyen – az elszámoltathatóság elvéből is következően.

4. KÖVETKEZTETÉS

A „munkavállaló ellenőrzése” komplex témakör. A technikai eszközökkel történő ellenőrzés is számos módon történhet. Ennek egyik módja a Rendeletben meghatározott követelmények érvényre juttatása (a Rendelet számos ellenőrzési kötelezettséget is tartalmaz), de a Rendeletben meghatározott követelmények érvényesítése során gyűjtött adatok nem csak a kiberbiztonsági követelmények érvényre juttatása céljából használhatóak fel, hanem más célra is, pl. a munkavégzéshez kapcsolódó jogi követelmények betartásának ellenőrzésére is, feltéve, hogy a munkáltató megfelelő indokot tud felmutatni és igazolni ezen addicionális ellenőrzési esetekre.

Mivel a munkavállaló ellenőrzése mindenképpen adatkezelési művelettel jár, hogy az adatkezelő (munkáltató) az adatkezelés megkezdése előtt a szükséges adatvédelmi dokumentumokat el kell készítse. Ezek közé tartozik az adatkezelési tevékenység nyilvántartása, az érintetteknek szóló adatkezelési tájékoztató, esetlegesen adatvédelmi hatásvizsgálat, illetve érdekmérlegelési teszt (ha az adatkezelés jogalapja az ún. jogos érdek). Az ellenőrzéseket előzetesen kidolgozott szabályzat alapján kell lefolytatni.