A munkáltató által biztosított IT eszközök magánhasználata

VFP2 KiberVéd - NIS2 Audit felkészítés szakmai iránymutatás 2026/5

VERZIÓKÖVETÉS

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

1. ÖSSZEFOGLALÁS

Jelen dokumentum a munkáltató által biztosított IT eszközök (hardver és szoftver) magáncélú használatát vizsgálja egy NIS2 kötelezett vállalkozás esetében. A legfontosabb tanulságok:

- A vállalati eszközök magánhasználata a Munka törvénykönyve[1] értelmében alapértelmezetten tilos, de a munkáltató engedélyezheti.
- A Kiberbiztonsági tv[2]. hatálya alá tartozó szervezetre vonatkozó biztonsági előírások nagymértékben megnehezítik a magánhasználatot.
- Amennyiben a munkáltató engedélyezi a magánhasználatot, az kiemelt adatvédelmi kockázatokkal jár, nagyon körültekintően kell eljárni adatvédelmi szakértő előzetes bevonásával.

2. PROBLÉMAFELVETÉS

A modern digitális munkakörnyezetben a szervezetek széles körű technológiai infrastruktúrát biztosítanak munkavállalóik számára (laptopok, okostelefonok, szoftverlicencek, e-mail fiókok, felhőalapú szolgáltatások, hálózati hozzáférés stb.) a hatékony és rugalmas munkavégzés érdekében. A funkcionális folyamatok (pl. HR, adózással kapcsolatos és egyéb nyilatkozatok) digitalizálása pedig szükségszerűen maga után vonja ilyen eszközök használatát, a munkavállaló magánszféráját érintő dokumentumoknak a munkáltató által biztosított eszközön való tárolását. Ezen túlmenően a munka és a magánélet közötti határok egyre inkább elmosódnak, különösen a távmunka és a hibrid munkavégzés terjedésével.

A kiberbiztonsági auditra való felkészülés során a magánhasználattal kapcsolatban az alábbi kérdéseket érdemes tisztázni:

- Használhatják-e a munkavállalók a cég által biztosított eszközöket magáncélra?
- Melyek a magánhasználat szempontjából releváns védelmi intézkedések?
- Milyen egyéb jogi előírásokat kell figyelembe venni a vállalati eszközök magánhasználata esetében?

3. IRÁNYMUTATÁS, AZ ALKALMAZANDÓ JÓ GYAKORLATOK

3.1 Használhatják-e a munkavállalók magáncélra a vállalati IT eszközöket?

A cég által biztosított számítástechnikai eszközök, szoftverek magánhasználata Munka törvénykönyvéről szóló 2012. évi I. törvény (továbbiakban, mint „Mt.") alapján alapértelmezetten tilos[3].

[1] 2012. évi I. törvény a munka törvénykönyvéről
[2] 2024. évi LXIX. törvény Magyarország kiberbiztonságáról

A munkáltató és a munkavállaló ettől eltérő megállapodást köthet.

Értelmezést igényel viszont a *„kizárólag a munkaviszony teljesítése érdekében”* fordulat a Mt-ben. Amennyiben a funkcionális folyamatok fentebb már említett digitalizálása nem tartozna ebbe a körbe, az ellentmondást okozna a magánhasználatot kategorikusan (kivételt nem ismerő módon) tiltó vállalati szabályozások esetén, illetve akkor is, ha ezek a kivételek nem szerepelnek a vállalati szabályzatokban.

3.2 Melyek a magánhasználat szempontjából releváns védelmi intézkedések?

Amennyiben szervezet vezetése úgy dönt, hogy engedélyezi a magánhasználatot a szervezet eszközein, ezt csak a 7/2024 (VI. 24.) MK rendelet vonatkozó előírásainak figyelembe vételével teheti meg.

A vonatkozó védelmi intézkedések bemutatását a 4.2 AA magánhasználat szempontjából releváns védelmi intézkedések c. fejezet tartalmazza.

A követelményrendszer természeténél fogva korlátozza a felhasználói tevékenységek körét. Alapelve nem az, hogy azt vizsgálja, hogy "Milyen magántevékenységeket tiltsunk le?", hanem azt, hogy "Mi az a minimális funkcionalitás, amire ennek a felhasználónak a munkájához szüksége van?". A legkisebb jogosultság (2.60) és a legszűkebb funkcionalitás (6.26.) elveinek alkalmazásával a szervezet gyakorlatilag minimálisra korlátozza azokat az eszközöket és jogosultságokat, amelyek a legtöbb általános magáncélú felhasználást lehetővé tennék (pl. programtelepítési jog, nem szabványos hálózati protokollok használata streaminghez vagy játékokhoz, hozzáférés a rendszerbeállításokhoz).

Ennek következtében a magánhasználat csak erősen korlátozott keretek között lehetséges, abban az esetben is, amennyiben a szervezet vezetése ezt engedélyezi.

3.3 Milyen feltételekkel engedélyezhető a magánhasználat?

Az IT eszközök magánhasználata számos adatvédelmi kérdést vet fel. Az informatikai eszközökkel kapcsolatos üzleti célú és magáncélú adatkezelések összemosása ugyanis jogi, és informatikai szempontból is rengeteg problémát és kérdést keletkeztet, főleg az ellenőrzési jogkör gyakorlása, a biztosított fizikai és logikai rendszerek feletti rendelkezési jog, az adatkezelés biztonsága érdekében kialakított szervezési és technikai intézkedések alkalmazhatósága tekintetében. A Nemzeti Adatvédelmi és Információszabadság Hatóság ugyanis a gyakorlatban csak nagy nehézségek árán teljesíthető követelményeket fektetett le (lsd. 4.3. pont alább) a kérdéskörben megengedő álláspontot képviselő munkáltatók részére és szinte minden vizsgált és közzétett esetben talált is bírságolásra okot adó körülményt.

A 7/2024 (VI.24.) MK rendelet által lefektetett, a vállalati IT környezetben a magánszférát jelentős mértékben korlátozó rendelkezések és a GDPR előírásainak összeegyeztetése IT eszközök magánhasználatának engedélyezése esetén kiemelt körültekintést igényel.

A döntés meghozatala előtt mindenképpen érdemes adatvédelmi szakértővel konzultálni és tekintettel arra, hogy az információbiztonsági követelmények teljesítése során jó eséllyel

[3] Mt. 11/A.§ (2) bekezdés

megvalósulhat a munkavállalók IT környezetének technikai eszközzel történő megfigyelése, adatvédelmi hatásvizsgálatra is szükség lehet.

3.4 Jó gyakorlat

Az indokolásban részletezett gyakorlati problémák figyelembevételével a munkavégzési célból biztosított számítástechnikai eszközök és szoftverek, tárhely (pl. laptop, levelezőrendszer, céges felhő tárhely) tekintetében a magáncélú adatkezelés tiltása, és az Mt. 11/A. §-a szerint alapértelmezett tiltó rendelkezéseinek alkalmazása javasolt, azzal hogy a Mt-nek a *„kizárólag a munkaviszony teljesítése érdekében”* fordulatát a munkáltató kellően alaposan értelmezi és határozza meg annak helyes tartalmát.

Arra az esetre, ha tiltás ellenére a felhasználó mégis magáncélú tartalmat tárol a szervezet számítástechnikai eszközén, javasoljuk, hogy a munkáltató zárja ki a kapcsolódó adatkezelés miatti felelősségét. A kilépő munkavállalókat kilépéskor nyilatkoztatni szükséges arról, hogy minden (a tiltás ellenére esetlegesen ott lévő) magáncélú tartalmat mentettek és eltávolítottak a szervezet hardver és szoftver eszközeiről.

4. INDOKOLÁS

4.1 Használhatják-e a munkavállalók magáncélra a vállalati IT eszközöket

Az Mt. 11/A. § (2) szerint:

> *A munkavállaló a munkáltató által a munkavégzéshez biztosított információtechnológiai vagy számítástechnikai eszközt, rendszert (a továbbiakban: számítástechnikai eszköz) – eltérő megállapodás hiányában – kizárólag a munkaviszony teljesítése érdekében használhatja.*

A fentebb már említettek szerint értelmezést igényel viszont a *„kizárólag a munkaviszony teljesítése érdekében”* fordulat a Mt-ben.

Alapvetően két értelmezés lehetséges ugyanis. Az első, szűkebb értelmezés szerint a „munkaviszony teljesítése” a munkakörből adódó feladatok ellátását jelenti (pl. jogtanácsos a peres iratok, vélemények elkészítése, értékesítő az ajánlatok elkészítésére, bérszámfejtő a munkabér elszámolásához szükséges teendőkre használhatja a számítástechnikai eszközt stb.).

A másik, tágabb értelmezés szerint a „munkaviszony teljesítése” nemcsak a fenti, „core” tevékenységeket foglalja magában, hanem a következőket is:

a) a munkáltató mint szervezet működtetéséhez (pl. új számítástechnikai eszköz igénylése, behajtási engedély igénylése – ez utóbbi nélkül a munkavállaló kiválóan el tudná látni a munkakörét – stb.) kacsolódó tevékenységek, valamint

b) a munkavállaló és a munkáltató közötti jogviszonnyal, vagy a munkáltató által ellátandó egyéb, funkcionális feladatokhoz kapcsolódó tevékenységek is, mint pl. adóelőlegek, adókedvezmények, társadalombiztosítási ellátások megállapításával, kifizetésével, a munkavégzéssel magával (pl. rendes szabadság vagy betegszabadság igénylése), a

munkavállalót megillető munkajogi kedvezményekkel (pl. gyermekek után járó pótszabadság, apasági szabadság stb.) stb. kapcsolatos tevékenységeket is.

Ez utóbbiakra (tehát a fenti a) és b) pontra) számos munkáltató alkalmaz digitalizált folyamatokat, azaz a munkavállalónak elektronikus úton (egy erre kifejlesztett alkalmazáson keresztül) *kell* az igénylést leadni, dokumentumot feltölteni; de ugyanígy elektronikus úton kap meg számos nyilatkozatot vagy dokumentumot a munkáltatótól (pl. a havi bérjegyzéket, az éves orvosi ellenőrzéshez szükséges nyomtatványt stb.). Számos esetben ezek az alkalmazások nem érhetők el másként csak a munkáltató eszközein (pl. VPN-en keresztül).

A gyakorlatban tehát a munkavállalóknak az esetek igen jelentős részében nincs más választása, mint a fenti tevékenységekhez kapcsolódó dokumentumokat (pl. táppénzes papírt, gyermek születési anyakönyvi kivonatát, magántulajdonú gépjármű forgalmi engedélyét stb.,) ideiglenesen a munkáltató által a munkavégzéshez biztosított számítástechnikai eszközön tárolni. Ha pedig ezeket a dokumentumokat (pl. a havi bérjegyzéket) a saját maga számára is meg akarja tartani, gyakorlatilag nincs más lehetősége, mint vagy külső eszközt csatlakoztatva a dokumentumokat letölteni vagy saját magán emailcímére elküldeni vagy egy magán tárhelyre feltölteni.

A munkáltatónak a belső szabályzatában tehát a fentebb körülírt eseteket meg kellene engednie (különösen azt, hogy az említett esetekkel összefüggésben a munkavállaló személyes adatokat tároljon a munkáltató eszközein és azok felett effektíve szabadon rendelkezzen), vagy biztosítania kell alternatív megoldást a munkaügyekhez kapcsolódó személyes dokumentumok beadásár (pl papír alapú adatszolgáltatás). Ezen felül azonban a munkáltatónak minden felelősséget ki kellene zárnia a magánhasználattal kapcsolatban, különösen az adatok bármilyen okból történő elvesztésének, vagy illetéktelenek általi hozzáférhetővé válásával kapcsolatos felelősséget (amennyiben azok nem olyan adatokat érintenek, amelyeket a munkavállaló – a fentiek szerint – okkal tárolhat a munkálttó által rendelkezésre bocsátott eszközökön).

4.2 A magánhasználat szempontjából releváns védelmi intézkedések

A 7/2024 (VI.24.) MK rendelet számos olyan rendelkezést tartalmaz, amelyek természetüknél fogva korlátozzák a felhasználói tevékenységek körét és nagyon nehezen alkalmazhatóak, ha a felhasználó magáncélra használja a szervezet eszközeit.

Az alábbi táblázat összefoglalja, hogy a 7/2024 (VI.24.) MK rendelet előírásai az egyes kulcsterületeken mennyiben teszik lehetővé a vállalati eszközök magánhasználatát.

Tevékenység / eszközkategória	**Irányadó követelmény(ek) (Azonosító és szöveg)**	**Következmény a magánhasználatra**	**Elsődlegesen kezelt szervezeti kockázat**	**Megjegyzés**
Szoftver				
Személyes szoftverek telepítése (játékok, segédprogramok)	{6.49.1.}[A]: "A szervezet: Megfogalmazza az EIR vonatkozásában a szervezetre érvényes követelményeket, amelyek meghatározzák a szoftverek felhasználó általi telepítési lehetőségeit." {6.31.2.}[J]: "Alkalmazza az alapértelmezett tiltás és a kivétel alapú engedélyezés szabályt a rendszeren futtatható szoftverek esetében." {6.47.1.}[A]: "A szervezet: Kizárólag olyan szoftvereket és olyan kapcsolódó dokumentációt használ, amelyek megfelelnek a rájuk vonatkozó szerződésbeli elvárásoknak, valamint a szerzői jogi vagy más jogszabályi	Tilos. Kizárólag kivételes eljárás keretében, külön engedéllyel lehetséges.	Kártevő/zsarolóvírus fertőzés, szoftverlicenc-sértések, rendszerinstabilitás.	

	előírásoknak."			
Web-alapú személyes e-mail/felhőtárhely használata	{13.4.1.}[A]: "A szervezet a viselkedési szabályaiba a következő korlátozásokat építi be: a közösségi média, közösségi oldalak és külső oldalak, valamint alkalmazások használatának korlátozása;" {2.75.1.2.}[A]: "A rendszer használatát megfigyelhetik, rögzíthetik, naplózhatják." {2.28.}[J]: "A szervezet a meghatározott információáramlási szabályokkal összhangban érvényesíti a jóváhagyott jogosultságokat a rendszeren belüli és a kapcsolódó rendszerek közötti információáramlás ellenőrzése során."	Korlátozott és felügyelt**.** A tevékenység naplózásra kerül, és az információáramlási kontrollok hatálya alá esik.	Adatszivárgás, adathalászat/kártevő bejutási vektor, a szervezeti adatok feletti kontroll elvesztése.	A korábban kifejtettek szerint bizonyos esetekben indokolt lehet ilyen alkalmazások használata, annak engedélyezése.
Közösségi média oldalak (pl. Facebook, X) használata	{13.4.1.}[A]: "A szervezet a viselkedési szabályaiba a következő korlátozásokat építi be: a közösségi média, közösségi oldalak és külső oldalak, valamint alkalmazások használatának korlátozása;" {13.4.2.}[A]: "a szervezeti információk közzétételének korlátozása nyilvános weboldalakon;"	Korlátozott és felügyelt. Tilos bármilyen nem nyilvános szervezeti információ közzététele.	Reputációs kár, adatszivárgás, termelékenység csökkenése, adathalászati vektor.	A „korlátozás” jelentheti azt is, hogy csak egyes munkavállalóknak (pl. a kommunikációért felelős szervezeti egység munkavállalóinak) biztosít hozzáférést a munkáltató a

				közösségi médiaoldalakhoz, mások számára viszont tiltja.
Vállalati hitelesítő adatok használata személyes fiókokhoz	**{13.4.3.}[A]:** "a szervezet által biztosított azonosító és hitelesítő adatok használatának korlátozása külső weboldalakon, illetve alkalmazásokban való fiókok létrehozásakor."	Szigorúan tilos.	Hitelesítő adatok kompromittálódása (credential stuffing), reputációs kockázat, biztonsági rés.	
Hardver				
Személyes USB-meghajtó/külső HDD csatlakoztatása	{11.14.1.}[A]: "A szervezet: Korlátozza vagy tiltja a szervezet által meghatározott típusú adathordozók használatát a szervezet által meghatározott EIR-eken vagy rendszerelemeken, a szervezet által meghatározott irányítási mechanizmusok alkalmazásával." {11.14.2.}[A]: "Megtiltja a hordozható adattároló eszközök használatát a szervezeti EIR-ekben, ha azoknak nincs azonosítható tulajdonosa." {18.8.3.1.}[A]: "Meghatározott időközönként átvizsgálja a rendszert, és valós időben ellenőrzi a külső forrásokból származó fájlokat a	Tilos. Az azonosítatlan adathordozók tiltottak; minden adathordozó kártevő-ellenőrzésen esik át.	Kártevő bejuttatása, jogosulatlan adateltávolítás, munkáltatói adatok jogosulatlan kimásolása, nem licencelt adatok bejuttatása.	Az adathordozók használatának *korlátozása* egyben a korlátozott használat engedélyezése is. A munkáltatónak döntést kell hoznia a tekintetben, hogy korlátozza vagy tiltja az említett eszközök csatlakoztatását, beleértve azt is, hogy kinek a számára korlátozza/ tiltja. A fentebb kifejtettek szerint a

	végpontokon, a hálózati belépési vagy kilépési pontokon a biztonsági szabályzatnak megfelelően, amint a fájlokat letöltik, megnyitják vagy futtatják."			munkáltatónak valamilyen módszert ajánlania kell a munkavállalók számára egyes releváns, elektronikus formában rendelkezésre álló dokumentumoknak a munkáltató rendszereibe való bejuttatás céljára.
Vállalati mobil eszköz használata személyes hívásokra/appokra	{2.113.1.}[A]: "A szervezet: Kialakítja a konfigurációs követelményeket, kapcsolódási követelményeket és alkalmazási útmutatót az általa ellenőrzött mobil eszközök számára, beleértve azokat az eseteket is, amikor ezek az eszközök a szervezet által ellenőrzött területen kívül helyezkednek el." {2.114.}[J]: "A szervezet teljes eszköztitkosítást vagy tárolóalapú titkosítást alkalmaz a meghatározott mobil eszközökön tárolt információk bizalmasságának és sértetlenségének védelme érdekében."	Erősen korlátozott. Az eszközön lévő minden adat a vállalati kontroll, titkosítás és potenciális távoli törlés hatálya alá esik. Nincs elvárható magánszféra.	Adatszivárgás, az eszköz kompromittálódása, ami hálózati hozzáféréshez vezethet, személyes adatok elvesztése.	Hangalapú hívások esetén legfeljebb az mutatható ki, hogy a használat nem *„kizárólag a munkaviszony teljesítése érdekében”* történt. A magánhasználat költségeinek megtérítésére vannak kialakult módszerek (pl. a híváslistán a munkavállaló

				megjelöli a magáncélú hívásokat).
Személyes perifériák (billentyűzet, egér, monitor) csatlakoztatása	{6.39.1.}[J]: "A szervezet: Meghatározott gyakorisággal, automatizált mechanizmusok segítségével vizsgálja a rendszerben található jogosulatlan hardver-, szoftver-, és firmware-elemek jelenlétét." {6.39.2.}[J]: "A jogosulatlan elemek észlelése esetén letiltja az ilyen elemek hálózati hozzáférését, izolálja a rendszerelemeket és értesíti a szervezet által meghatározott személyeket vagy szerepköröket."	Korlátozott. "Jogosulatlan hardverként" észlelhető, ami hálózati izolációt válthat ki.	Hardveralapú kártevők (pl. BadUSB), rendszerinstabilitás.	
Általános Tevékenység				
Személyes fájlok (fotók, zenék, dokumentumok) tárolása	{17.81.}[J]: "A szervezet megóvja a meghatározott tárolt, illetve archivált (at rest) adatok bizalmasságát és sértetlenségét a feldolgozás vagy továbbítás alatt álló adatokkal megegyező szinten." {17.82.}[J]: "A szervezet meghatározott rendszerelemek vagy adathordozók esetében kriptográfiai mechanizmusokat alkalmaz a szervezet által meghatározott	Nem javasolt és kockázatos**.** A fájlok megfigyelés, biztonsági mentés és az eszköz újrahasznosításakor történő biztonságos törlés tárgyát képezik. Nincs garancia a magánszférára vagy a helyreállításra.	Jogi/bizonyítási felelősség, tárhelyfogyasztás, kártevő-vektor (fertőzött fájlok).	A fentebb kifejtettek szerint ez a tilalom csak olyan fájlokra vonatkozhat, amelyek semmilyen módon nem kapcsolhatóak a munkaviszonyhoz. Az esetleges tiltás vagy törlés szempontjából ugyanakkor

	tárolt vagy archivált adatok jogosulatlan felfedésének és módosításának megelőzésére." {7.35.1.}[A]: "A szervezet: Meghatározott gyakorisággal mentést készít az EIR-ben tárolt felhasználói szintű információkról, összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal." 1 {11.8.1.}[A]: "A szervezet: A meghatározott, biztonságos törlési technikákkal és eljárásokkal törli az EIR meghatározott adathordozóit a leselejtezés, a szervezet ellenőrzési körén kívülre kerülés, vagy az újra felhasználásra való kibocsátás előtt."			figyelembe veendő, hogy egy számítástechnikai eszközön a dokumentumok között nem igazán lehet különbséget tenni azok belső tartalma alapján (egy pdf dokumentum lehet a havi bérjegyzék, de lehet a munkáltató bizalmas információja is, és ennek eldöntésében a fájl neve sem feltétlenül mérvadó, hiszen az bármikor átnevezhető).
Bármilyen tevékenység végzése a vállalati hálózaton	{2.75.1.2.}[A]: "A rendszer használatát megfigyelhetik, rögzíthetik, naplózhatják." {4.13.1.}[A]: "A szervezet: Meghatározott gyakorisággal felülvizsgálja és elemzi a rendszer naplóbejegyzéseit a nem megfelelő vagy szokatlan tevékenységre utaló jelek és	Felügyelt. Minden tevékenység naplózásra kerül, és "nem megfelelő vagy szokatlan tevékenység" szempontjából felülvizsgálható.	Minden biztonsági kockázat. A magánszféra hiányának alapelve.	

	az ilyen tevékenységek lehetséges hatásai szempontjából." {18.13.1.}[A]: 18.13. A szervezet: 18.13.1. Monitorozza a rendszert, hogy észlelje: 18.13.1.1. A támadásokat és a potenciális támadásokra utaló jeleket összhangban a meghatározott felügyeleti célokkal; 18.13.1.2. Az engedély nélküli helyi, hálózati és távoli kapcsolatokat. 18.13.2. Azonosítja a rendszer jogosulatlan használatát a meghatározott technikák és módszerek alkalmazásával. 18.13.3. Aktiválja a belső felügyeleti képességeket vagy telepíti a felügyeleti eszközöket: 18.13.3.1. az egész rendszerre kiterjedően a szervezet által meghatározott információk gyűjtése érdekében; illetve 18.13.3.2. a rendszeren belül ad-hoc módon meghatározott helyeken a szervezet által meghatározott információk gyűjtése érdekében. 18.13.4. Elemzi az észlelt			

	eseményeket és rendellenességeket			

4.3 A magánhasználat adatvédelmi kérdései

Az IT eszközök magánhasználata számos adatvédelmi kérdést vet fel. Publikált határozataiban[4] a Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: NAIH) ugyanis a gyakorlatban csak óriási nehézségek árán teljesíthető követelményeket fektetett le a kérdéskörben megengedő álláspontot képviselő Adatkezelők részére, és szinte minden vizsgált és közzétett esetben talált is bírságolásra okot adó körülményt. Meg kell jegyezni, hogy a NAIH álláspontja sok esetben megkérdőjelezhető. A munkáltató azonban csak akkor számíthat sikerre a NAIH-hal szemben, ha koherens érvrendszert állít szembe a Hatóság álláspontjával.

A NAIH/2019/51/11. sz. határozatban kifejtett hatósági álláspont szerint a céges postafiókban lévő magán levelezés tekintetében a munkáltató és a munkavállaló között a GDPR 26. cikk szerinti közös adatkezelői jogviszony áll fent. - Tehát közös adatkezelői megállapodást kellene kötniük. - Na de a munkavállaló a saját magánlevelezése tekintetében jellemzően nem is tekinthető a GDPR értelmében vett adatkezelőnek. - *Ilyen esetekben tehát egy igen sajátos együttes adatkezelési helyzet áll elő, amely esetben a munkáltató mindenképpen adatkezelőnek minősül, a munkavállaló pedig – jogi értelemben legalábbis – nem feltétlenül."* Ugyanakkor *"a munkáltatóé az adatkezelés jogszerűségéért való elsődleges felelősség",* úgy, hogy ezekbe az adatokba a munkáltató jogszerűen nem is nézhet bele.

A NAIH álláspontja szerint a munkavállalói magáncélú adatainak kezelésére egy munkáltató általánosságban nem rendelkezik jogszerű céllal és ennélfogva jogalappal. Azokat kizárólag – teljes rendszere részeként tárolni, archiválni, és üzletmenet folytonosságának biztosítása, adatbiztonsági követelményei teljesítése céljából biztonsági mentésével együtt menteni jogosult. Ilyenkor az említett adatkezelési célok – kényszerűen – ezekre az adatokra is kiterjedhetnek, a kényszerűen adatkezelővé váló üzemeltető jogalapja ezekre a tevékenységekre pedig a jogos érdeke (GDPR 6. cikk (1) f) pont) lehet, vagy az adatbiztonságot, üzembiztonságot biztosító tevékenység – közérdekű feladatot ellátó szervezetek esetén – a közérdekű feladata ellátáshoz szükséges, járulékos adatkezelésként értelmezhető (GDPR 6. cikk (1) e) pont). Azonban mindkét jogalap esetén, azon kívül hogy rengeteg többlet adminisztratív tevékenységet keletkeztetnek az Adatkezelőnek (érdekmérlegelések, tájékoztatók), igen „kellemetlen" körülmények hátráltathatják az általában szükség szerint gyors, diszkrét, azonnali beavatkozások hatékonyságát – ugyanis az érintettek jogosultak tiltakozni (GDPR 21. cikk) az adatkezelési tevékenység ellen, valamint élhetnek egyéb érintetti jogaikkal (hozzáféréshez való jog GDPR 15. cikk, törléshez való jog GDPR 17. cikk).

---

[4] NAIH 421-19/2013/H számú határozat (https://www.naih.hu/files/421_2013_hatarozat_anonim.pdf)
NAIH 2015/1402/H számú határozat (https://www.naih.hu/files/2355_2014_H_hat_anonim.pdf)
NAIH/2019/769 sz. határozat (https://www.naih.hu/files/NAIH-2019-769-hatarozat.pdf)
NAIH/2019/51/11 sz. határozat (https://www.naih.hu/files/NAIH-2019-51-hatarozat.pdf)
NAIH/2020/34/3 sz. határozat (https://naih.hu/files/NAIH-2020-34-3-hatarozat.pdf)
NAIH/2020/2074/2.sz. határozat (https://naih.hu/files/NAIH-2020-2074-hatarozat.pdf)
A Nemzeti Adatvédelmi és Információszabadság Hatóság tájékoztatója a munkahelyi adatkezelések alapvető követelményeiről https://www.naih.hu/files/2016_11_15_Tajekoztato_munkahelyi_adatkezelesek.pdf 25-32. oldal

Tiltakozás esetén a Munkáltató addig nem folytathatja az adatkezelést, amíg nem mérlegeli az érintett által felhozott érveket, és saját jogainak, érdekeinek az érintett jogait korlátozó hatásait, ami jelentősen megtörheti egy ellenőrzés dinamizmusát. Az egyéb érintetti joggyakorláshoz pedig praktikusan a Munkáltatónak biztosítania kell, hogy a munkavállaló a betekintést, majd a törlést kontrollálhassa, akár írásban, személyesen jelezhesse, melyik állomány minősül magáncélú tartalomnak, majd lementhesse maga részére azt, és törölhesse. Munkáltatónak saját érdekei képviseletét is biztosítani kell a válogatás alatt, biztosítva ezzel a védett adatai illetéktelen kimentésének megakadályozását, valamint a sokszor többféle különböző időállapotban, és terjedelemben rendelkezésre álló mentéseiből, archív állományaiból is ki kellene válogatni, el kellene távolítani ilyekor ezeket az adatokat, ez pedig informatikailag nagyon erőforrásigényes feladat, azon felül, hogy ezeknek az állományoknak az integritása, teljessége értelemszerűen sérül ilyenkor.

A magánhasználat engedélyezése a gyakorlatban nagyon nehezen kivitelezehető. Definíció szerint adatkezelő az, aki meghatározza az adatkezelés célját és eszközeit. A vázolt esetben (a munkáltató számítástechnikai eszközeinek magáncélra történő használata erre vonatkozó tiltás ellenében) munkáltató semmilyen módon nem határozza meg az adatkezelés célját és eszközeit, azt teljesen a munkavállaló határozta meg (n.b. a munkáltató tudta ellenére). A nem engedélyezett magáncélú használat – nevéből is következően – egy jogellenes helyzet, amit ugyan a munkáltató megtűrhet, de felelősséggel nem tartozhat érte.

Az az álláspont, miszerint „a munkavállalói magáncélú adatainak kezelésére egy munkáltató általánosságban nem rendelkezik jogszerű céllal és ennélfogva jogalappal”, értelmezhetetlen, hiszen a fentebb kifejtettek szerint a munkáltató az akarata ellenére van bizonyos adatok birtokában, de az adatok birtoklása még nem jelent adatkezelői minőséget, mert ez utóbbi döntési kompetenciát takar. Az adatkezelő (tehát az, aki a döntést hozta arról, hogy mit akar tárolni a munkáltatója eszközein vagy milyen egyéb adatkezelési műveletet akar végrehajtani a munkáltatója eszközeinek felhasználásával) nem más, mint a munkavállaló; és akinek az adatkezelői minősége valószínűleg egy jogellenes döntéssel párosul.

Az adatbiztonság (GDPR 32. cikk) tk. az egyetlen olyan jogi kötelezettség, ami magából a GDPR-ból származik, így a kérdéses kötelezettség a GDPR 6. cikk (1) bek. c) pontja („jogi kötelezettség”) alá esik (hiszen minden adatkezelőt ugyanúgy terhel). Tekintettel arra, hogy a fentiek szerint elkerülhetetlen, hogy a munkavállaló „privát” adatai ne kerüljenek be a munkáltató rendszereibe, illetve az is, hogy valamilyen módon a munkáltatói rendszerek és a munkavállaló rendszerei (pl. elektronikus levelezőrendszere vagy tárhelye) ne kerüljenek kapcsolatba. Mivel egy fájl neve önmagában semmit nem mond sem a tartalmáról, sem a „tulajdonos” személyéről, a lehetséges megoldások szempontjából releváns kérdés, hogy van-e olyan technikai megoldás, amivel visszavonhatatlanul meg lehet címkézni egy fájlt (pl. "magán" és "hivatalos"). Ha igen, a mentések, a törlések, keresések nem érintenék egyik vagy másik kategóriát (feltéve, hogy más szoftverek képesek felismerni egy fájl tulajdonságait), vagy éppenséggel célzottan lehetne felkutatni az ilyen fájlokat. Ha volna ilyen kitörölhetetlen attribútuma egy fájlnak, egy átnevezéssel sem lehetne megváltoztatni egy fájl jellemző tulajdonságát (tehát a munkáltató üzleti titkát tartalmazó dokumentum egy esetleges átnevezés ellenére is munkáltató üzleti titkát tartalmazó dokumentum maradna).

Hasonlóképpen, ha technikailag lehetséges, hogy pl. bizonyos mappákat a rendszer nem ellenőriz, akkor ki lehetne jelölni egy bizonyos mappát, ahol a munkavállaló a saját fájljait tárolhatja (amire a munkáltató jogi felelőssége nem terjedne ki).

5. FORRÁSOK

5.1 Jogszabályok

- 2012. évi I. törvény a Munka Törvénykönyvéről
- 2024. évi LXIX. törvény Magyarország kiberbiztonságáról (Kiberbiztonsági tv.)
- A Miniszterelnöki Kabinetirodát vezető miniszter 7/2024. (VI. 24.) MK rendelete a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről
- Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) 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 (általános adatvédelmi rendelet) (GDPR)

5.2 NAIH határozatok

- NAIH/2019/51/11. sz. határozat
- NAIH 421-19/2013/H számú határozat
- NAIH 2015/1402/H számú határozat
- NAIH/2019/769 sz. határozat
- NAIH/2019/51/11 sz. határozat
- NAIH/2020/34/3 sz. határozat
- NAIH/2020/2074/2.sz. határozat
- A Nemzeti Adatvédelmi és Információszabadság Hatóság tájékoztatója a munkahelyi adatkezelések alapvető követelményeiről