

A munkavállalók személyes adatainak kezelése

I. A Hatósághoz érkező érintetti kérelmek, panaszbeadványok, konzultációs megkeresések egyik jelentős csoportját alkotják a munkahelyi adatkezeléseket érintő beadványok.

Ezek témája eléggé változatos, így található közte

- álláspályázatra jelentkezés során történő adatkezeléssel,
- alkalmassági tesztekkel,
- feddhetetlen előélet igazolásával,
- fegyelmi vétségekkel kapcsolatos beadványok, valamint
- a leggyakoribb problémaforrás, a munkahelyi ellenőrzés valamelyik típusával kapcsolatos panaszok.

II. A munkahelyi ellenőrzéssel összefüggő adatkezelések közzé sorolható a:

- munkavállalók kamerás megfigyelése,
- internethasználat,
- e-mail fiók,
- céges eszközök (telefon, laptop) ellenőrzése,
- különböző beléptetőrendszerek és beléptetési gyakorlatok,
- GPS navigációs rendszerek és
- biometrikus rendszerek alkalmazásával folytatott ellenőrzés.

III.1. Kiválasztási folyamat során történő adatkezelések gyakori kérdései:

- Elsőként az adatkezelés jogalapját kell megvizsgálni.

Munkaviszonyban a munkavállaló és a munkáltató egymással alá-fölérendeltségi viszonyban van, ezért ebben a jogviszonyban az érintetti hozzájárulás nem elfogadott azokban az esetekben, amikor a munkavállalót a hozzájárulás megtagadása miatt hátrány éri vagy érheti, hiszen a hozzájárulás megadása nem lesz önkéntes. A munkáltatók ezért munkaviszonyban személyes adatot jellemzően a szerződéses jogalap, jogszabályi kötelezettség, illetve jogos érdek jogalap alapján kezelhetik.

Mivel az álláshely megpályázása során még nem áll fenn ez az alá-fölérendeltségi viszony, nem zárható ki, hogy a kiválasztási folyamat során történő egyes adatkezelések esetében a hozzájárulás legyen az alkalmazott jogalap, azonban a legbiztosabb talán a munkáltató jogos érdekére alapítani az adatkezelést, ez a jogos érdek megfelelő érdekmérlegeléssel támasztandó alá.

- Fontos kérdés, hogy a kiválasztási eljárás során milyen személyes adatok ismerhetők meg a jelentkezőről. Ezt az adatkört az adattakarékosság elve figyelembevételével lehet meghatározni. Természetesen nem mindig tudhatja

előre a munkáltató, hogy milyen adatokat fog megadni magáról a pályázó, azonban mindenképpen tekintettel kell lennie az adattakarékosság elvére, vagyis csak olyan adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen. Ezt a követelményt, ha összekapcsoljuk a célhoz kötött adatkezelés, valamint a korlátozott tárolhatóság elvével, további megállapításokat tehetünk a vizsgált adatkezeléssel kapcsolatban:

- az ilyen célból gyűjtött adatokat kizárólag a kiválasztási folyamat lebonyolításához szabad felhasználni,
- a kiválasztási eljárás lezárásakor – amikor megvan, hogy kinek tesz ajánlatot a munkáltató – az eredménytelenül pályázók személyes adatait meg kell semmisíteni.

Ezen törlési kötelezettség alól kivételt képez az az eset, amikor a pályázó kifejezett, egyértelmű és önkéntes hozzájárulása alapján a munkáltató megőrizheti a pályázó személyes adatait, azonban fontos, hogy valóban csak a pályázó kifejezett kérésére kerüljön erre sor, valamint ez az adatkezelés sem tarthat korlátlan ideig, 1 éven túl szükségtelen megőrizni ezeket a pályázati anyagokat.

- Mind erről, mind az álláspályázat során folytatott adatkezelésről természetesen megfelelő előzetes tájékoztatást kell nyújtania az adatkezelőnek a GDPR 13. cikke alapján.

III.2. Hatósági erkölcsi bizonyítvány bekérése:

A Hatóság álláspontja szerint nem várható el a munkavállalótól, hogy már a jelentkezés alkalmával megküldje az erkölcsi bizonyítványát, még akkor sem, ha az adott munkakörre egyébként megalapozottan kérhető a feddhetetlenség igazolása.

További probléma szokott lenni a megfelelő jogalap hiánya. Tekintettel arra, hogy büntetett előéletre vonatkozó adatról van szó, ezért különleges adatnak minősül az erkölcsi bizonyítvány tartalma. A munkaviszonyban a munkáltatók egyrészt a GDPR 6. cikk (1) bekezdés c) pontja és az adatkezelés részleteit szabályozó törvényi felhatalmazás alapján kezelhetik a munkavállalók bűncselekményre, a büntetlen előélet megállapítására vonatkozó személyes adatait. Ilyen jogszabályi felhatalmazást tartalmaz számtalan foglalkozás esetében a munkakört szabályozó jogszabály, pl. bíró, ügyész, közjegyző, fegyveres biztonsági őr, ingatlanközvetítő, könyvvizsgáló stb. esetében, vagy pl. a hitelintézetekről és a pénzügyi vállalkozásokról szóló törvény értelmében a vezető állású személyek tekintetében. Hasonló törvényi feltételeket állapít meg a munka törvénykönyvéről szóló 2012. évi I. törvény (a továbbiakban: Mt.) 44/A. §-a a tizennyolcadik életévét be nem töltött személy nevelését, felügyeletét, gondozását, gyógykezelését végző munkáltató által foglalkoztatott személyek vonatkozásában.

A fenti törvényi felhatalmazások hiányában a munkáltatók a munkavállalók feddhetetlenségére vonatkozó személyes adatait az általános adatvédelmi rendelet 6. cikk (1) bekezdés f) pontja szerinti jogos érdek alapján és a 9. cikk (2) bekezdés b) pontja szerinti feltétel teljesülése esetén kezelhetik. Az ott előírt garanciákat a bűnügyi nyilvántartási rendszerről, szóló 2009. évi XLVII. törvény

(Bnyt.) biztosítja. A munkáltatóknak a jogos érdek jogalapjára történő hivatkozáshoz szükséges érdekmérlegelést végezniük. Az azonban kiemelendő, hogy nem fogadható el, hogy a munkáltató általános jelleggel és minden munkavállalóra kiterjesztve hatósági erkölcsi bizonyítványt kérjen. Ugyanis önmagában az a tény, hogy a munkavállaló a munkáltatónál jelentős értéket képviselő eszközökkel fog dolgozni vagy a munkáltató üzleti titkaihoz és bizalmas információihoz lesz hozzáférése, nem elegendő ok az ilyen típusú ellenőrzésre.

Fontos továbbá, hogy csupán az erkölcsi bizonyítvány bemutatása kérhető a munkavállalótól, arról a munkáltató másolatot nem készíthet. A hatósági erkölcsi bizonyítványról készített másolat ugyanis nem rendelkezik bizonyító erővel arról, hogy hiteles másolata egy érvényes hatósági közokiratnak, így a másolat nem alkalmas a benne szereplő adatok hiteles megállapítására, kezelése sérti a célhoz kötött adatkezelés elvét.

IV.1. Munkahelyi ellenőrzés céges eszközökön

A munkahelyi ellenőrzés egyre nagyobb mértékben érinti a munkavállalókat, hiszen jelentős időt töltenek a munkahelyen, ez a napnak jellemzően az a része, amikor minden mást is intézni tud az ember, ezért a munkavállalók időnként munkaközi szünetben igyekeznek magánügyeiket elintézni, melyhez gyakran a munkáltató által biztosított rendszereket, eszközöket használják. Az utóbbi évek technológiai fejlődése lehetővé tette a munkáltatók számára, hogy a munkavégzés hatékonyságának növelése érdekében számos újítást építsenek be a munkafolyamatokba, ezekkel az eszközökkel pedig tapasztalataink szerint élnek is a munkáltatók. Így ma már mindennaposnak számít, hogy a munkáltató céges mobiltelevont, laptopot ad a munkavállalóinak, távoli hozzáférést biztosít a levelezőrendszerhez, munkáltatói szerverhez, mellyel lehetővé teszi, hogy ne csak a munkahelyen legyen végezhető a munka, melynek azonban az a hátrányos következménye figyelhető meg a munkavállalók szempontjából, hogy elmossa a munka és a magánélet közötti határt.

A munkáltatók által folytatott ellenőrzési tevékenységek során a GDPR szabályai irányadóak elsősorban, ezek közül csak említés szintjén emelném ki a jogszerű cél szükségességét, vagyis személyes adat csak jogszerű cél elérése érdekében kezelhető, a már említett célhoz kötöttség elvét, valamint az adattakarékosság elvét. Hiszen amennyiben a megjelölt adatkezelési cél, mint legitim adatkezelési cél elfogadható is, az adattakarékosság elve szerint vizsgálni kell, hogy a jogszerű adatkezelési célt egyéb eszközzel észszerű, illetve arányos módon el lehet-e érni. Az adattakarékosság elvéről szóló (39) preambulumbekkezdés továbbá kimondja azt is, hogy a személyes adatoknak a kezelésük céljára alkalmasoknak és relevánsoknak kell lenniük.

Ha tehát az alkalmazott eszköz valójában nem is alkalmas a cél elérésére, vagy ha nem feltétlenül szükséges a cél eléréséhez, illetve nem arányos a vele megvalósuló magánszféra korlátozással, esetleg rendelkezésre áll olyan módszer, mely kevésbé sérti az érintettek magánszféráját, akkor a Hatóság rendszerint megállapítja az adatkezelés jogszerűtlenségét. Mindezek mellett természetesen ki kell emelni az alapelveknek való megfelelés igazolásának képességét előíró elszámoltathatóság elvét.

A GDPR mellett másik fontos jogszabály munkahelyi ellenőrzés szempontjából az Mt., mely sok más jogszabályhoz hasonlóan szintén módosult a GDPR-nak való megfelelés érdekében a 2019-es Salátatörvénnyel, mely módosítás jelentős változásokat hozott a munkahelyi ellenőrzés témakörében.

Az Mt. 11/A. § (1) bekezdése értelmében a munkavállaló a munkaviszonnal összefüggő magatartása körében ellenőrizhető. Ennek keretében a munkáltató technikai eszközt is alkalmazhat, melyről a munkavállaló-t előzetesen írásban köteles tájékoztatni.

A módosítás értelmében 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. Vagyis a korábbi főszabályt megfordította a jogalkotó és azt tette alapértelmezetté, hogy a magáncélú használat kizárt, ez alól csak a felek megállapodása jelenthet kivételt. Tehát minden munkavállalóval külön-külön meg kell állapodnia a munkáltatónak. Ebben a megállapodásban azonban mindenképpen célszerű részletesen szabályozni a magáncélú használat feltételeit és az alkalmazott korlátozásokat (például az alkalmazott tartalomszűrésekről, illetve, hogy mikor engedélyezett a magáncélú használat).

A 11/A. § (3) bekezdése alapján a munkáltató az ellenőrzés során a munkaviszony teljesítéséhez használt számítástechnikai eszközön tárolt, a munkaviszonnal összefüggő adatokba tekinthet be. A következő bekezdés értelmében pedig ilyen munkaviszonnal összefüggő adatnak minősül magának a magáncélú használatra vonatkozó szabályok megtartásának ellenőrzéséhez szükséges adat. A munkáltató tehát az ellenőrzés során olyan mértékben tekinthet be az adatokba, hogy meg tudja állapítani, hogy az adat magáncélú-e vagy sem. Az Mt. nem szűkíti le ennek az ellenőrzésnek a lehetőségét a munkáltató által biztosított eszközökre, vagyis megfelelő keretek között alkalmazható lehet ez a szabály a manapság egyre gyakrabban előforduló azon esetekben, amikor a munkavállaló saját eszközét használja munkavégzésre („bring your own device”).

A munkahelyi ellenőrzéseket az arányosság megtartásával, az adattakarékosság elvéből is adódóan célhoz kötötten, a fokozatosság elvére figyelemmel lépcsőzetes módon szükséges megvalósítani.

Így például az ellenőrzés első lépéseként az e-mail cím és a levél tárgyának az ellenőrzése is elegendő lehet, hiszen bizonyos esetekben már pusztán az e-mail cím felépítéséből és az e-mail tárgyból is lehet látni azt, hogy az magáncélú e-mail lesz, és ezért nem szükséges megismerni az e-mail tartalmát. Emellett, ha például a munkáltató nem engedélyezi az e-mail-fiók magáncélú használatát, és az ellenőrzés pusztán arra terjed ki, hogy megállapítsa azt, hogy a munkavállalók betartották-e ezt a munkáltatói rendelkezést, akkor szintén elegendő az e-mail címének és tárgyának megtekintése, és nem szükséges a levél tartalmának megismerése, hiszen munkajogi jogkövetkezményeket már ezen tény megállapítása alapján is alkalmazhat a munkavállalókkal szemben.

A magánjellegű levelekkel kapcsolatban szükséges kiemelni azt is, hogy az ilyen e-mailek tartalmát a munkáltató főszabály szerint nem jogosult megismerni, arra csak rendkívül nyomós okból, kivételes esetben kerülhet sor.

A tisztességes adatkezelés elvéből olyan követelmény is származik, hogy az ellenőrzés során főszabályként biztosítani kell a munkavállaló jelenlétét, hiszen ezáltal biztosítható, hogy az érintett ne váljon kiszolgáltatottá az adatkezelővel, sem más személlyel szemben. Az adatalany mindvégig alanya kell, hogy maradjon a személyes adatok kezelésével járó folyamatnak, és nem válhat annak pusztá tárgyává. A munkavállaló jelenléte nélküli ellenőrzés ezért alapvetően ellentétes a tisztességes adatkezelés elvével.

A munkavállaló előzetes tájékoztatása és – személyes, vagy ha ez nem biztosítható, akkor meghatalmazottjának, képviselőjének – jelenléte az ellenőrzésnél azért is szükséges, mert a munkavállaló és harmadik személyek különböző személyes adatai lehetnek benne a levelezőrendszerben, amelyek kezelésére a munkáltató – a személyes adat jellege ellenőrzésén túl – nem jogosult. Ha az ellenőrzés során a munkavállaló – képviselője, meghatalmazottja – jelen van, és jelezheti valamely személyes adatot tartalmazó e-mail tartalmának megtekintése előtt, hogy az magáncélú személyes adatokat tartalmaz, akkor ezzel biztosítható, hogy a munkáltató ne sértse meg ezt a tilalmat.

Az ellenőrzés körülményeitől függően ugyanakkor elképzelhetőek olyan helyzetek, amikor a munkavállaló személyes jelenléte objektív okokból nem biztosítható. A Hatóság egyes rendkívüli esetekben elfogadhatónak tartja, 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 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-mail-fiókjához, 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, 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.

IV.2. E-mail postafiók ellenőrzése

A Hatóság több határozatában is foglalkozott ezzel a kérdéssel és általánosságban megállapította, hogy abban az esetben, amikor a munkavállaló használja az e-mail-fiókot, számítástechnikai eszközöket – függetlenül attól,

hogy a munkáltató egyébként megtiltja vagy engedélyezi a magáncélú használatot – a munkáltató által biztosított eszközökben, rendszerekben tárolt személyes adatok tekintetében a munkáltató maga is adatkezelési tevékenységet végez.

Amennyiben az adatkezelés a munkavégzéssel összefügg, a munkavállaló lényegében a munkáltató, mint adatkezelő nevében jár el, e tevékenysége, mint adatkezelői tevékenység, a munkáltatónak tudható be.

Azonban amikor a munkavállaló a munkáltató által biztosított eszközökön magáncélú tevékenységet folytat és így saját és a legtöbb esetben harmadik személyek személyes adatait kezeli, már bonyolultabb a helyzet. Ekkor ugyanis az adatkezelés célját nem a munkáltató határozza meg, hanem a munkavállaló, aki ezáltal adott esetben maga is adatkezelővé válik a harmadik személyek személyes adatai tekintetében. Ő dönt a személyes adatnak a rendszerbe, eszközre kerüléséről, és amíg a birtokában, rendelkezése alatt van az eszköz, addig dönthet annak törléséről, egyéb felhasználásáról. Ugyanakkor ezen személyes adatok tekintetében is – különösen a „céges e-mail-fiók” esetében – a rendszer működtetése továbbra is a munkáltató feladata és hatásköre, és a személyes adatokat tároló eszköz feletti rendelkezési jogát sem veszíti el a munkáltató, aki a magáncélú adatok tekintetében ezért adatkezelő lesz.

A munkáltató adatkezelői minősége azért sem kérdőjelezhető meg ebben az esetben, mert még, ha kifejezett engedélyén és tudtán kívül kerülnek is rendszereibe személyes adatok, azok egyrészt a saját adatkezelései tekintetében is eljáró személyek révén kerülnek oda, másrészt adatkezelési műveleteket végez rajtuk – mindenekelőtt tárolja azokat, és adott esetben hozzáfér ezen személyes adatokhoz.

Ez a következtetés az Mt. említett módosítását követően, tehát abban az esetben is igaz marad, ha az Mt. értelmében kizárt a munkáltató eszközeinek magáncélú használata, mivel az adatkezelés mibenléte és az adatkezelői minőség alapvetően ténykérdés, így a vonatkozó rendelkezés csak a felelősség kérdésében vezethet eltérő eredményre.

Alapvető fontosságú, hogy amennyiben a munkavállaló magáncélú személyes adatai vonatkozásában a munkáltató adatkezelőnek minősül, ez nem jelenti egyúttal azt is, hogy az ilyen személyes adatok kezelése a munkáltató részéről minden esetben jogszerű. Hiszen, ha a munkáltató oldalán nem azonosítható ezen adatok kezelésének semmilyen jogszerű célja, illetve a 6. cikk (1) bekezdése szerinti jogalapja, akkor az ilyen adatok kezelése nem lesz jogszerű, a munkáltató részéről az ilyen személyes adatok nem kezelhetők. A jogalap nélküli adatkezelésnek pedig elsődlegesen az az általános jogszerű következménye, hogy a munkáltató – amint értesül ezen adatok kezelésének tényéről – megszünteti azok kezelését, azaz törli ezeket a rendszeréből, az általa biztosított eszközökről. Ugyanakkor az adatok törlése mint adatkezelési művelet csak a munkavállaló érdekeinek figyelembe vételével, és az adatkezelés tisztességességére vonatkozó követelménynek a betartásával valósítható meg jogszerűen.

A munkáltatónak mint adatkezelőnek ennek megfelelően tájékoztatnia kell a munkavállalót a tervezett adatkezelési műveletről és lehetőséget kell biztosítania számára, hogy az adatok kezelését (törlését) kontrollálhassa, és – ha a kérdéses adatok törlése esetén azok a munkavállaló számára a továbbiakban már nem lennének elérhetők – az adatokat a maga számára saját eszközre mentse. A munkáltatónak az ilyen adatmentést joga és kötelezettsége felügyelni annak érdekében, hogy az valóban csak a magáncélból kezelt adatokra korlátozódjon. Egy olyan eljárás és mechanizmus kialakítása és megvalósítása szükséges tehát, ahol lehetőség szerint mindkét fél kontrollálja az adatok „szétválogatásának” folyamatát, és ennek során az általa jogszerűen nem kezelhető adatokat csak az adat e minőségének megállapításához, a folyamat ellenőrzéséhez legszükségesebb körre korlátozódjon.

IV.3. Céges eszközök ellenőrzése

A munkáltatók számára egyre több olyan eszköz áll rendelkezésre, mely hatékony segítséget nyújt rendszereik és egyéb érdekeik védelmére, így pl. adatvesztést megakadályozó eszközök, fenyegetéskezelő rendszerek, többfunkciós tűzfalak, a használt programok és eszközök használatának láthatatlan megfigyelését lehetővé tevő szoftverek, a munkavállalók tevékenységét naplózó eszközök stb., melyek a munkavállalók magánéletébe potenciálisan egyre nagyobb behatolást jelentenek.

Az adatkezelés jogalapja a jogos érdek lehet, azonban a fentiekben felsorolt és más hasonló eszközök alkalmazásának szándéka esetében az adatkezelőnek szükséges megvizsgálnia azt, hogy nem aránytalan-e a reakció, melyet a munkáltatók az elérni kívánt cél érdekében végrehajtanak, illetve mérlegelendő, hogy van-e olyan módszer, ami szintén biztosítja a munkáltató, illetve pl. ügyfelei adatai biztonságát, azonban kisebb behatolást jelent a munkavállalók magánszférájába.

Az Adatvédelmi Munkacsoport 2017-es WP249-es véleménye pl. helyes gyakorlatnak tartja, ha a munkáltató elkülönült hozzáférést biztosít a munkavállaló számára, amely nem áll munkáltatói megfigyelés, ellenőrzés alatt. Ilyen megoldás lehet például ingyenes vezeték nélküli internet-hozzáférés biztosítása különálló készülékeken. Ezen túlmenően számítógép vagy laptop esetében elkülönült fiókok vagy partíciók kialakítása segíthet abban, hogy a munkavégzési célú és a magánjellegű fájlokat elkülönítetten lehessen ugyanazon a gépen kezelni.

Az azonban mindenképpen fontos, hogy megfelelő szabályzatban a kellő mértékben tájékoztassa a munkáltató a munkavállalókat az ellenőrzés kereteiről, az adatokhoz való hozzáférés szabályairól, ezáltal lehetővé téve a munkavállalók számára, hogy viselkedésüket úgy alakítsák, hogy ne figyeljék meg őket, amikor a munkahelyi informatikai eszközöket magáncélra használják.

Még nagyobb kockázatot rejt magában mind a munkáltató, mind a munkavállaló szempontjából az otthoni, a távoli munkavégzés, illetve az Mt. említett módosítása által is nevesített saját eszközök munkacélú használata. Hiszen

lehetetlen ezen számítástechnikai eszközök esetében ugyanazon szervezeti és biztonsági intézkedéseket megtenni, mint a munkahelyen telepített rendszer esetében. Ezen kockázatok számos esetben arra sarkallják a munkáltató-t, hogy olyan eszközöket vegyen igénybe a munkavállalók ellenőrzése során, mint pl. egérmozgások, billentyűzetleütések rögzítése, képernyőképek véletlenszerű vagy meghatározott időközönkénti mentése, webkamerákból származó felvételek gyűjtése, amelyek használata azonban nem összeegyeztethető a szükségesség-arányosság, célhoz kötöttség elvével, továbbá a jogos érdek jogalap sem igazán állja meg ez esetben a helyét.

Megoldás lehet erre:

- közös céges szerver alkalmazása az adattárolásra, mely jelszóval érhető el, vagy
- a céges dokumentumok, e-mailek stb. tárolása egy távolról elérhető applikációban, mely elérhető a munkáltató részére, ugyanakkor kizárja a magánszférát érintő tartalmakhoz (pl. képek, filmek, privát levelezés) való hozzáférést.

A céges telefon használata kapcsán is felmerülhet a munkáltató jogos érdeke az ellenőrzésre, azonban ez az ellenőrzési módszer is sértheti a munkavállalók magánszféráját. Ebben a körben két esetet különböztethetünk meg:

HA *nem engedélyezett a magánhasználat*: a Munka tv. módosítása folytán ugyebár ez az alapeset. Tisztább helyzetet teremt egy esetleges ellenőrzés alkalmával, hiszen, ha a hívás kizárólag munkaviszonnyal összefüggésben kezdeményezhető, akkor egyértelmű a munkavállaló részére, hogy a munkáltató a kimenőhívások hívószámát és adatait ellenőrizheti, melynek célja a magáncélú hívások szűrése, bizonyítása.

Azonban, HA *engedélyezett a magánhasználat*: a fentiekhez képest jóval bonyolultabb helyzettel van dolgunk, hiszen a kétféle típusú hívás nehezen különíthető el. Ebben nyújt segítséget a Hatóság azon gyakorlati megoldási javaslata, miszerint:

- két előhívó szám alkalmazásával egyértelműen elkülöníthető a magáncélú telefonbeszélgetés a munkahelyi hívástól, előbbi ezáltal nem ismerhető meg és annak költségeinek viselésére kötelezhető a munkavállaló, az utóbbi esetben azonban a hívások ellenőrzés alá vonhatóak, a költségeket pedig a munkáltató viseli; vagy

- a munkáltató az előzetesen kikért hívásrészletezőt átadja a munkavállaló részére, kérve, hogy saját maga különítse el a beszélgetéseket, "felismerhetetlenné téve" a magánbeszélgetések adatait.

V. Végezetül tanulmányozásra érdemes a munkáltatói ellenőrzés kapcsán született két fontos, az Emberi Jogok Európai Bíróságán a GDPR hatályba lépése előtt született ítéletet.

Ugyan mindkét ítélet az Emberi Jogok Európai Egyezményének 8. cikkének, a magán és családi élet tiszteletben tartásához való jog értelmezését tartalmazza, azonban

mivel az EJEB ítéletei minden államot köteleznek, ezért irányadónak tekinthetők az előadás során tárgyalt esetekben is. Az egyik ilyen döntés a **Bărbulescu kontra Románia** ítélet, melyben a dián olvasható kritériumokat támasztotta az EJEB a munkavállaló ellenőrzésének jogszerűsége kérdésében:

- Előzetesen és világosan tájékoztatták-e a munkavállaló-t 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 kevésbé korlátozó olyan ellenőrzés, mellyel a kívánt cél szintén elérhető lett volna?
- Mik a megfigyelés következményei a megfigyelés a munkavállalóra nézve?
- Az ellenőrzés belső rendje tartalmaz-e megfelelő biztosítékokat – pld előzetes figyelmeztetés – a munkavállaló tevékenységének, levelezésének ellenőrzése kapcsán?
- Biztosított-e a jogorvoslat lehetősége?

Ez a fenti teszt nagyon hasznos lehet a munkáltatók számára annak felmérése során, hogy megfelelően alakította-e ki a munkahelyi ellenőrzéssel kapcsolatos gyakorlatát.

A másik ítélet a **Libert kontra Franciaország** ügyben született, melyből az a jó gyakorlat emelendő ki, miszerint annak eldöntését, hogy a munkavállaló által használt, munkáltató által rendelkezésre bocsátott laptopon, levelezőfiókban tárolt adatok személyes adatnak tekintendők-e, nagyban segíti, ha azt a privát jelzéssel látja el a munkavállaló, ezzel egyértelművé téve, hogy arra nem terjedhet ki a munkáltató ellenőrzése.