



A Nemzeti Adatvédelmi és Információszabadság Hatóság

tájékoztatója

a munkahelyi adatkezelések alapvető követelményeiről

Bevezetés

A Nemzeti Adatvédelmi és Információszabadsághoz (a továbbiakban: Hatóság) számos olyan panasz, illetve konzultációs beadvány érkezik, mely a munkahelyi adatkezelések területét érinti.

A munkahelyi adatkezelések több csoportba sorolhatóak. Egyrészt különbség tehető abban a tekintetben, hogy létező munkaviszonyról beszélünk-e, vagy sem. A munkaviszony létesítése előtt megvalósuló adatkezelés alapvetően az azt megelőző pályáztatási eljárással, valamint a munkakörre való alkalmasság vizsgálatával összefüggésben valósul meg. A munkaviszony megszűnését követően szintén történik adatkezelés, amikor is például a munkáltató jogszabályi kötelezettség alapján nyilvántartja a volt munkavállalója személyes adatait. A munkaviszony fennállása alatti adatkezelések között is differenciálhatunk. Egyrészt például társadalombiztosítási, adózási okokból szükséges személyes adatok kezelése, de ekkor is felmerülhet az alkalmassággal kapcsolatban adatkezelés. Szintén gyakori adatkezelésként jelenik meg az egyre jobban elterjedő visszaélés-bejelentési rendszerekkel összefüggő adatkezelés. További adatkezelés a munkavégzéssel összefüggésben keletkezik: minősítési, fegyelmi vétségekkel és büntetésekkel kapcsolatos eljárások során. Ezen túlmenően a munkavállaló ellenőrzésével kapcsolatban is felmerül személyes adatok kezelése. Ez utóbbi esettel kapcsolatban elmondható, hogy a technika fejlődésével egyre gyakoribb a munkavállalók technikai eszközökkel történő ellenőrzése. Ebbe a körbe tartozik többek között a munkavállalók kamerás megfigyelése, elektronikus levelezésük, valamint internethasználatuk ellenőrzése, a rendelkezésükre bocsátott úgynevezett „céges mobiltelefon” használatának ellenőrzése, a GPS navigációs rendszer alkalmazása során történő ellenőrzés, illetve a biometrikus rendszerek alkalmazásával megvalósuló ellenőrzés. A Hatósághoz érkező beadványok nagy számban a munkavállalók technikai ellenőrzésével együtt járó adatkezeléseket érintik.

Jelen állásfoglalás célja, hogy útmutatóul szolgáljon mind a munkavállalók, mind a munkáltatók számára, és megismerjék, hogy a munkavégzést érintő adatkezelések, különösen a munkáltatói ellenőrzéssel összefüggő adatkezelések esetében milyen követelményeknek kell érvényesülniük.

A Hatóság a tájékoztatóban szereplő alapvető szempontokkal kívánja segíteni az adatkezelőket a jogszerű adatkezelés kialakításában.

A 2018. május 25-étől Magyarországon is alkalmazandó új adatvédelmi rendelet a Hatóság előzetes elemzése alapján jelentős változásokat nem fog eredményezni az ügyek tartalmi megítélésében.

Tartalomjegyzék

Bevezetés	1
Tartalomjegyzék.....	2
I. Általános szabályok.....	4
1. A munkahelyi adatkezelés során érvényesülő adatvédelmi alapelvek	4
1.1. A célhoz kötött adatkezelés elve.....	4
1.2. A szükségesség-arányosság elve	6
2. Az adatkezelés jogalapja.....	7
2.1. Az érintett hozzájárulása	7
2.2. Törvényen alapuló adatkezelés.....	8
2.3. A munkáltató jogos érdekén alapuló adatkezelés	8
2.4. Az Mt. és az Infotv. szabályai az adattovábbítás jogalapjával kapcsolatban	11
3. Az előzetes tájékoztatás követelménye	12
4. Adattovábbítás külföldre.....	13
4.1. Adattovábbítás az EGT-n belül.....	13
4.2. Adattovábbítás az EGT-n kívülre	13
5. Az adatvédelmi nyilvántartásba való bejelentési kötelezettség.....	14
6. A munkahelyi adatkezelésekkel kapcsolatos joghatósági kérdések	15
II. Egyes speciális munkahelyi adatkezelések	18
1. Az állás pályázatra jelentkezés és a magán-munkaközvetítés	18
1.1. „Anonim álláshirdetések”.....	18
1.2. Az állás pályázatra jelentkező munkavállaló valamely közösségi oldalon létrehozott profiljának megtekintése	18
1.3. A pályázatok, önéletrajzok megőrzése.....	19
1.4. A pályázati anyagok kezelésével kapcsolatos egyéb adatvédelmi követelmények.....	20
1.5. A magán-munkaközvetítő által kezelhető adatok	20
2. Alkalmassági vizsgálatok	21
2.1. Általános adatvédelmi követelmények	21
2.2. A munkáltató által előírt alkalmassági vizsgálatok követelményei	21
2.3. A munkaviszony fennállta alatt végzett munkahelyi tréningek adatvédelmi követelményei	22
3. A munkavállalók feddhetetlen előéletének igazolása	22
4. A munkavállalók munkaviszonnal összefüggő magatartásának ellenőrzése	23
4.1. Munkahelyi kamerás megfigyelés.....	23

4.2. A munkáltató által a munkavállaló rendelkezésére bocsátott e-mail fiók használatának ellenőrzése	25
4.2.1. Előzetes intézkedések.....	25
4.2.2. Adatvédelmi követelmények.....	26
4.3. A munkáltató által a munkavállaló rendelkezésére bocsátott laptop ellenőrzése	28
4.3.1. Előzetes intézkedések.....	28
4.3.2. Adatvédelmi követelmények.....	29
4.3.3. Speciális követelmények, ha a laptop magáncélú használatát nem engedélyezi a munkáltató.....	29
4.3.4. Egyéb adatvédelmi követelmények.....	30
4.4. Az internethasználat ellenőrizhetősége	30
4.5. A „céges mobiltelefon” használatának ellenőrizhetősége	31
4.5.1. Előzetes intézkedések.....	31
4.5.2. A nem engedélyezett magáncélú telefonhasználat ellenőrzése.....	31
4.5.3. Az engedélyezett magáncélú telefonhasználat ellenőrzése.....	32
4.5.4. További adatvédelmi követelmények.....	32
5. GPS navigációs rendszer alkalmazhatósága	33
6. Biometrikus rendszerek alkalmazhatósága	34
6.1. A biometrikus rendszer.....	34
6.2. Előzetes adatvédelmi követelmények.....	35
7. A belső visszaélés-bejelentési rendszer (whistleblowing) adatvédelmi követelményei	36
7.1. A visszaélés-bejelentési rendszer.....	36
7.2. Követelmények.....	36
7.3. A kezelhető személyes adatok köre és ideje.....	37
7.4. Adatvédelmi követelmények.....	37
III. Jogszabályjegyzék	39
IV. Egyéb joganyagok	40

I. Általános szabályok

1. A munkahelyi adatkezelés során érvényesülő adatvédelmi alapelvek

Az Infotv.¹ és az Mt. egyaránt tartalmazza az adatvédelem alapelveit, amelyek kiemelten fontosak ahhoz, hogy bizonyos, a munkáltató rendelkezései szerint kialakított adatkezelések jogszerűek legyenek. A munkáltatóknak ezen alapelvekre figyelemmel kell kialakítaniuk az adatkezelési körülményeket. Ezért érdemes áttekinteni, hogy az egyes alapelvekből milyen gyakorlati követelmények származnak a munkahelyi adatkezelésekkel kapcsolatban.

1.1. A célhoz kötött adatkezelés elve

Infotv.	Mt.
<p>4. § (1) bekezdés <i>Személyes adat kizárólag meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében kezelhető. Az adatkezelésnek minden szakaszában meg kell felelnie az adatkezelés céljának, az adatok felvételének és kezelésének tisztességesnek és törvényesnek kell lennie.</i></p>	<p>10. § (1) bekezdés <i>A munkavállalótól csak olyan (...) adat közlése kérhető, amely személyiségi jogát nem sérti, és a munkaviszony létesítése, teljesítése vagy megszűnése szempontjából lényeges. A munkavállalóval szemben csak olyan alkalmassági vizsgálat alkalmazható, amelyet munkaviszonyra vonatkozó szabály ír elő, vagy amely munkaviszonyra vonatkozó szabályban meghatározott jog gyakorlása, kötelezettség teljesítése érdekében szükséges.</i></p>

Ezen alapelvből fakadó gyakorlati követelmények:

- Az adatkezelés célját az adatok rögzítését megelőzően, világosan és egyértelműen meg kell határozni. A célnak kellően részletesnek kell lennie annak érdekében, hogy azonosíthatóak legyenek a szükséges adatkezelési műveletek és az alkalmazandó további garanciális szabályok. A cél meghatározásának részletezettsége alapvetően az adatkezelés körülményeitől és a kezelt személyes adatok fajtáitól függ. Általánosságban elmondható, hogy a túl tág, általános fogalmakkal körülírt cél nem felel meg e követelménynek.
- A munkáltatónak minden egyes adatkezelés esetében adatkezelési célonként külön-külön meg kell határozni azt a jogot, amelynek gyakorlásához szükséges valamely személyes adat kezelése, vagy azt a kötelezettséget, amelynek teljesítése szükségessé teszi az adatkezelést.

¹ A tájékoztató III. pontjában („Jogsabályjegyzék”) megtalálható valamennyi, a tájékoztatóban hivatkozott magyar jogszabály pontos megjelölése. A tájékoztató szövegében a jogszabályok rövidített elnevezései szerepelnek.

- A célhoz kötött adatkezelés elve a hivatkozott Mt. 10. § (1) bekezdésben is megjelenik. Ez azt jelenti, hogy a munkáltatónak minden adatkezeléséhez célt kell rendelnie. Azaz személyes adat csak akkor kezelhető, ha az lényeges, ha az adat kezelése nélkül a munkaviszony létesítése, fenntartása, megszűnése nem lenne lehetséges. A munkáltatónak az adatkezelései jogszerűségét elsősorban azzal kell alátámasztania, hogy minden adatkezelése vonatkozásában igazolni tudja az adatkezelés célját, és azt, hogy az adatkezelés a cél eléréséhez szükséges.
- Mindezek alapján a munkáltató köteles a munkavállalóktól kért adatok körét előre oly módon meghatározni, hogy az adatok csakis a munkaviszony létesítéséhez, fenntartásához, megszűnéséhez kapcsolódjanak. A munkavállalókat tájékoztatni kell arról, hogy a tőlük kért adatok, velük szemben alkalmazott vizsgálatok milyen információként szolgálhatnak a munkáltató számára. Minden olyan adat kérése, mely nem ad lényeges tájékoztatást a munkaviszony létesítése, fenntartása, megszüntetése szempontjából, indokolatlanul korlátozza a munkavállalók magánszféráját, személyes adataikkal való rendelkezés jogukat – különösen akkor, ha a munkáltató az adatszolgáltatás megtagadása esetén kilátásba helyezi például a munkaviszony létesítésének megtagadását.
- Amennyiben az adatokon eltérő célokból végeznek műveleteket, akkor a célokat egyenként definiálni kell. Továbbá az adatkezelésnek minden szakaszában meg kell felelnie az adott adatkezelési célnak, és tilos adatokat kezelni olyan újabb célból, amely összeegyeztethetetlen az eredetivel. Így például, ha a munkáltató a munkaszerződés alapján rendelkezésére álló adatokat fel akarja használni belső képzés szervezésére (így különösen a munkavállalók nevét, munkakörét, végzettségét), akkor ez a munkajogviszonyból fakadó, korábbi adatkezelésekhez képest új adatkezelési cél, amelyet külön definiálni kell.
- Bizonyos munkakörök esetén munkaviszonyra vonatkozó szabály² alkalmazási vizsgálatot írhat elő. Ebben a körben különösen fontos szerepe van a tisztességes adatkezelés követelményének, ugyanis a munkáltató – például a munkahelyi felvételi eljárás során – kizárólag olyan kérdést intézhet a munkavállalók felé, amely a munkaviszony, alkalmazási vizsgálat szempontjából releváns, és az érintettek személyiségi jogait – így a személyes adatok védelméhez való jogukat – nem sérti. Az adatkezelés tisztességes volta az emberi méltóság védelmével áll szoros kapcsolatban, a tisztességtelen adatkezelési gyakorlat az érintetteket nem csak személyes adataikhoz fűződő jogában, de emberi méltóságukban is súlyosan sértheti.

² Mt. 13. §-a értelmében az Mt. „*alkalmazásában munkaviszonyra vonatkozó szabály a jogszabály, a kollektív szerződés és az üzemi megállapodás, valamint az egyeztető bizottságnak a 293. §-ban foglaltak szerint kötelező határozata.*”

1.2. A szükségesség-arányosság elve

Infotv.	Mt.
<p style="text-align: center;">4. § (2) bekezdés <i>Csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas. A személyes adat csak a cél megvalósulásához szükséges mértékben és ideig kezelhető.</i></p>	<p style="text-align: center;">9. § (2) bekezdés <i>A munkavállaló személyiségi joga akkor korlátozható, ha a korlátozás a munkaviszony rendeltetésével közvetlenül összefüggő okból feltétlenül szükséges és a cél elérésével arányos</i></p> <p style="text-align: center;">11. § (1) bekezdés <i>A munkáltató a munkavállalót csak a munkaviszonnyal összefüggő magatartása körében ellenőrizheti. A munkáltató ellenőrzése és az annak során alkalmazott eszközök, módszerek nem járhatnak az emberi méltóság megsértésével. A munkavállaló magánélete nem ellenőrizhető.</i></p>

Ezen alapelvnek elsődlegesen a munkáltatói ellenőrzéseknél van jelentősége. Az alapelvből fakadó gyakorlati követelmények:

- Az alkalmazott eszköznek alkalmasnak kell lennie a cél elérésére, vagyis csak akkor lehet ellenőrzést folytatni, ha egyértelmű, hogy az alkalmazni kívánt eszköz, módszer által az ellenőrzés útján a védeni kívánt munkáltatói érdekek, jogok sérelme megelőzhető.
- Az ellenőrzés csak a szükséges mértékű adatkezeléssel járhat. Ez egyszerre jelenti az adatkezelés időbeni korlátozottságát, és azt is, hogy a személyes adatokat csak a szükséges esetben, és csak az arra feljogosított személyek használhatják fel.
- Az ellenőrzés csak a munkával összefüggésben történhet, a munkavállalók magánélete nem ellenőrizhető. Ezzel kapcsolatban fontos kiemelni, hogy a munkavállalókat a munkahelyen is megilleti a magánélethez való jog, és ezt a munkáltatónak tiszteletben kell tartania. A „munkahelyi magánélet” tipikus színterei az ebédlő, az öltöző, a pihenőhelyiség, a mosdók.
- Az ellenőrzésnek minden esetben a munkavállalók emberi méltóságának tiszteletben tartásával kell történnie. Az ellenőrzés nem irányulhat a munkavállalók megfélemlítésére, megalázására, zaklatására, zavarására, és ezeket nem is eredményezheti.

2. Az adatkezelés jogalapja

A magyar és az uniós jogszabályi rendelkezések alapján különböző jogalapok alkalmazhatóak annak érdekében, hogy az adatkezelés jogszerű legyen³, amelyek közül a munkahelyi adatkezelés során alapvetően három jogalap jöhet szóba: az érintett hozzájárulása, törvényi felhatalmazás, illetve a munkáltató jogos érdekén alapuló adatkezelés.

2.1. Az érintett hozzájárulása

A hozzájárulás⁴ jogalapjának legfontosabb feltétele, hogy annak önkéntesnek, azaz mindenfajta külső befolyástól mentesnek kell lennie. Az Adatvédelmi Munkacsoport⁵ több dokumentumában⁶ kifejtett álláspontjára⁷ támaszkodva a Hatóság gyakorlata szerint is a hozzájárulás jogalként csak akkor jöhet szóba, ha valódi választási lehetőség áll az érintett rendelkezésére, és nem áll fenn a megtévesztés, a megfélemlítés, a kényszerítés vagy más jelentős negatív következmény veszélye a hozzájárulás megtagadása esetén. Az önkéntesség hiányában az adatkezelő nem rendelkezik megfelelő jogalappal az adatkezeléshez. A munkavégzésre irányuló jogviszonyokban azonban nem értelmezhető a hozzájárulás önkéntessége: a munkáltató és a munkavállaló közötti alá-fölérendeltségi viszonyban, ha az alkalmazott a hozzájárulását megtagadja, ez anyagi vagy nem anyagi természetű hátrányt okozhat neki.⁸

Az érintett hozzájárulására, mint jogalapra, a munkahelyi adatkezelések esetében tehát csak kivételesen lehet hivatkozni, alapvetően akkor, amikor egyértelmű, hogy az adatkezelés során feltétel nélküli „előnyöket” szerez a munkavállaló, és nem érheti őt semmilyen hátrány az adatkezelés megtagadása esetén.

A hozzájárulás megfelelő jogalap lehet, ha az adatkezelésre nem a munkaviszonnyal összefüggésben kerül sor, vagyis ha az adatkezelés a munkáltatói jogok gyakorlásával nem áll kapcsolatban. Például egy munkáltató egy futóversenyre csapatot szervez, amelyhez a munkáltatónak továbbítania kell a szervezők részére azon munkavállalóinak az adatait, akik részt vennének a versenyen, mivel a munkáltató állja a nevezés költségeit. Emellett a munkáltató pólókat is biztosít a versenyre, ezért a munkavállalók pólóméretét továbbítania kell a pólót készítő vállalkozás részére. Ez két különböző adattovábbítást jelent, és mindkettőhöz egymástól függetlenül önkéntes hozzájárulást tud adni a munkavállaló anélkül, hogy ennek bármilyen következménye lenne a munkaviszonyára nézve.

³ Infotv. 5-6. §-a, Adatvédelmi Irányelv 7. cikk f) pontja.

⁴ Infotv. 3. § 7. pont: „*hozzájárulás: az érintett akaratának önkéntes és határozott kinyilvánítása, amely megfelelő tájékoztatáson alapul, és amellyel félreérthetetlen beleegyezését adja a rá vonatkozó személyes adat – teljes körű vagy egyes műveletekre kiterjedő – kezeléséhez.*”

⁵ Az Adatvédelmi Munkacsoport az adatvédelemmel, valamint a magánélet védelmével kapcsolatos kérdésekkel foglalkozó, független európai tanácsadó szerv.

⁶ A tájékoztató IV. pontjában („Egyéb joganyagok”) megtalálható az Adatvédelmi Munkacsoport joganyagainak pontos megnevezése és elérhetősége.

⁷ Így például a hozzájárulás fogalom-meghatározásáról szóló 15/2011. számú vélemény.

⁸ Így például az Adatvédelmi Munkacsoport 15/2011. számú véleményében kimondta, hogy: „*ha a munkavállaló hozzájárulását kéri, és a hozzájárulás megtagadása valós vagy lehetséges sérelem merül fel, akkor a hozzájárulás nem érvényes sem a 7. cikk, sem a 8. cikk értelmében, mivel azt nem önkéntesen adták. Nem beszélhetünk hozzájárulásról, ha a munkavállaló számára nem áll fenn a visszautasítás lehetősége.*”

A hozzájárulás jogalapjának egyik speciális esete az Infotv. 6. § (3) bekezdésében⁹ megfogalmazott kivétel, amelynek alapján 16 éven aluli kiskorúakat érintő adatkezelések jogszerűségéhez szükséges a szülő beleegyezése. Az Mt. ezzel szemben más szabályokat tartalmaz a kiskorúak munkavállalásával kapcsolatban.¹⁰ A munkahelyi adatkezelések során párhuzamosan figyelemmel kell lenni mind az Infotv., mind az Mt. sajátos szabályaira. Így például az Mt. 34. § (3) bekezdése alapján nem csak a szülő beleegyezése szükséges a munkaszerződés megkötéséhez, hanem a gyámhatóság engedélye is.

A fent kifejtettek alapján elmondható tehát, hogy a munkáltatói adatkezelések esetében a hozzájárulás mint jogalap csak szűk körben jelenik meg, amikor is ténylegesen fennállhat az önkéntesség.

2.2. Törvényen alapuló adatkezelés

A munkahelyi adatkezelések egy jelentős része törvényi rendelkezésen alapul: vagy olyan törvényi előírás, amely kötelezővé teszi az adatkezelést, vagy olyan jogszabályon, amely csupán lehetővé teszi az adatkezelést. Mindkét esetben előfordul, hogy az adott törvény az adatkezelés valamennyi körülményét szabályozza, de olyan jogszabály által nevesített adatkezelés is létezik, amelynél a törvény az adatkezelés részleteit, körülményeit nem határozza meg, azokat az adatkezelőre bízta.

Törvényen alapuló, kötelező adatkezelést széles körben rendelnek el az adókötelezettségre, társadalombiztosításra vonatkozó jogszabályok. Ezen jogszabályok rendelkezései a munkáltatók és a munkavállalók számára kötelezettségként jelennek meg, vagyis ezek ténylegesen kötelező adatkezelések.

Ezen túlmenően a munkaviszonyra is irányadóak lehetnek olyan törvények, amelyek az adatkezelést a munkáltató számára lehetővé teszik. Ebbe a körbe tartozik például a munkáltatói visszaélés-bejelentési rendszerrel, illetve a munkáltató ellenőrzési jogosultságával összefüggő adatkezelés a munkavégzés tekintetében. Azonban ezek nem tekinthetők klasszikusan törvényi felhatalmazáson alapuló adatkezeléseknek, hanem közelebb állnak a munkáltató jogos érdekén alapuló adatkezelések csoportjához, hiszen a munkáltatók több-kevesebb mozgástérrel rendelkeznek az adatkezelési körülmények meghatározásában.

2.3. A munkáltató jogos érdekén alapuló adatkezelés

A munka világában az érintett hozzájárulása helyett – a fenti szűk esetkört leszámítva – más jogalapok alkalmazása indokolt. Az Adatvédelmi Munkacsoport kifejtette, hogy a jogszerű

⁹ Infotv. 6. § (3) bekezdés: „a 16. életévét betöltött kiskorú érintett hozzájárulását tartalmazó jognyilatkozatának érvényességéhez törvényes képviselőjének beleegyezése vagy utólagos jóváhagyása nem szükséges.”

¹⁰ Mt. 34. § (2)-(3) bekezdése értelmében „munkavállaló az lehet, aki a tizenhatodik életévét betöltötte. Ettől eltérően munkavállaló lehet – az iskolai szünet alatt – az a tizenötödik életévét betöltött tanuló, aki nappali rendszerű képzés keretében tanulmányokat folytat. A gyámhatóság engedélye alapján a jogszabályban meghatározott kulturális, művészeti, sport-, hirdetési tevékenység keretében a tizenhatodik életévét be nem töltött személy is foglalkoztatható.”

adatkezelésnek nem csak a hozzájárulás lehet az egyetlen jogalapja, hanem az Adatvédelmi Irányelv 7. cikkében szereplő többi jogalap is alkalmazható az adatkezelők számára.

Az Európai Bíróság a C-468/10. és C-469/10. sz. egyesített ügyekben hozott ítéletére¹¹ tekintettel ezen jogalapok közül kiemelt szereppel rendelkezik az Adatvédelmi Irányelv¹² 7. cikk f) pontja. Ezen rendelkezés értelmében személyes adat kezelhető abban az esetben is, ha a munkahelyi adatkezelés a munkáltató – kivételesen harmadik fél – jogos érdekének érvényesítéséhez szükséges, kivéve, ha ennél az érdekeknél magasabb rendűek a munkavállalók személyes adatai védelméhez és a magánéletük tiszteletben tartásához való joguk. A 7. cikk f) pontjában szereplő jogalap egyik fő jellemzője az, hogy ez a munkavállalók hozzájárulásától függetlenül jogszerűvé teheti a munkáltató adatkezelését, feltéve, ha a munkáltató jogos érdeke arányosan korlátozza a munkavállalók személyes adatok védelméhez való jogát, magánszféráját.

A munkáltatóra hárul azon kötelezettség, hogy belső szabályzatban vagy más írásbeli dokumentumban kidolgozza ezen jogalap alkalmazásával végzett adatkezeléseit. Fontos garanciális szempont, hogy a munkáltató írásban rögzítse ezen az jogalap alkalmazásával együtt járó adatkezelési körülményeket, hiszen a munkavállalók így tudnak meggyőződni arról, hogy a szóban forgó munkahelyi adatkezelés valóban arányosan korlátozza a jogaikat. Emellett a Hatóság vagy a bíróság is így tudja ellenőrizni, vizsgálni azt, hogy a munkáltató adatkezelése megfelelt-e az adatvédelmi követelményeknek.

A jogalap alkalmazása során a munkáltatónak két követelményre kell figyelemmel lennie. Egyrészt ezen jogalap alkalmazásakor a magyar jogszabályi előírásokat, így különösen az Mt. és az Infotv. rendelkezéseit kell alapul vennie. Másrészt ezzel egyidejűleg el kell végeznie az érdekmérlegelési tesztet. Az Adatvédelmi Munkacsoport véleménye¹³ támpontot jelenthet ahhoz, hogy

- milyen szempontok alapján lehet meghatározni a munkáltatói jogos érdeket,
- mire kell a munkáltatónak figyelemmel lennie az érintetti érdekek, jogok meghatározása során,
- melyek az érdekmérlegelési teszt elvégzése során megfontolandó kulcsfontosságú tényezők,
- melyek lehetnek például az adatkezelők által alkalmazott olyan intézkedések, amelyek biztosítják az érintettek magánszférájának és személyes adatainak védelmét.

Az érdekmérlegelési teszt elvégzése során a munkáltatónak számos szempontra figyelemmel kell lennie, ezért a Hatóság egy lehetséges foratókönyvet javasol, amely mellett természetesen elfogad más módszereket is ennek a tesztnek az elvégzésére.

- *1. lépés:* a munkáltatónak a tervezett adatkezelés megkezdése előtt át kell tekintetnie, hogy a célja elérése érdekében feltétlenül szükséges-e személyes adat kezelése: rendelkezésre állnak-e olyan alternatív megoldások, amelyek alkalmazásával személyes adatok kezelése nélkül megvalósítható a tervezett cél.

¹¹ A tájékoztató IV. pontjában megtalálható az Európai Unió Bírósága döntésének pontos megnevezése és elérhetősége.

¹² A tájékoztató III. pontjában megtalálható az Adatvédelmi Irányelv pontos megnevezése. A tájékoztató szövegében a rövidített elnevezés szerepel.

¹³ Az adatkezelő 95/46/EK irányelv 7. cikke szerinti jogszerű érdekeinek fogalmáról szóló 6/2014. számú vélemény

- *2. lépés:* a munkáltatói jogos érdek lehető legpontosabb meghatározása (így különösen az Mt. 10. § (1) bekezdésének figyelembe vételével).
- *3. lépés:* annak meghatározása, hogy mi az adatkezelés célja, milyen személyes adatok, meddig tartó adatkezelését igényli a jogos érdek.
- *4. lépés:* annak meghatározása, hogy a munkavállalóknak mik lehetnek az érdekeik az adott adatkezelés vonatkozásában (például azok a szempontok, amelyeket a munkavállalók felhozhatnak az adatkezeléssel szemben).
- *5. lépés:* annak meghatározása, hogy miért korlátozza arányosan a munkáltatói jogos érdek – és az ennek alapján végzett adatkezelés – a 4. lépésben meghatározott munkavállalói jogokat, várakozásokat. A munkáltatónak az érdekmérlegelés során segítséget nyújthatnak azok az alapelvek, amelyeket a tájékoztató 2. pontjában a Hatóság már kifejtett. Az érdekmérlegelésen alapuló munkahelyi adatkezelések esetében többek között az alábbi garanciák biztosíthatják az adatkezelés szükségesség-arányosságát (természetesen más garanciális intézkedések is szóba jöhetnek):
 - *A fokozatosság elvének érvényesülése.* Ennek a garanciának elsődlegesen a munkáltatói ellenőrzésekkel együtt járó adatkezelések esetén van jelentősége. A munkáltatónak a munkavállalók munkavisztonnyal összefüggő magatartásának ellenőrzése körében lehetőleg olyan módszert kell választania, amely nem jár együtt személyes adat kezelésével. Ha nincs ilyen, akkor a magánszférát legkevésbé korlátozó módszert kell alkalmaznia, amelynek nyomán korlátozott körben ismer meg személyes adatokat.
 - *A munkavállaló jelenlétének biztosítása.* Ugyancsak a munkáltatói ellenőrzések keretében van szerepe ezen garanciának. Amennyiben az ellenőrzés körülményei nem zárják ki ennek lehetőségét, akkor biztosítani kell, hogy a munkavállaló jelen lehessen az ellenőrzés során (így például a felvételek visszanezésekör vagy az e-mail elolvasásakor).

2.4. Az Mt. és az Infotv. szabályai az adattovábbítás jogalapjával kapcsolatban

Infotv.	Mt.
<p>5. § (1) bekezdés <i>Személyes adat akkor kezelhető, ha</i> <i>a) ahhoz az érintett hozzájárul, vagy</i> <i>b) azt törvény vagy – törvény felhatalmazása alapján, az abban meghatározott körben – helyi önkormányzat rendelete közérdeken alapuló célból elrendeli (a továbbiakban: kötelező adatkezelés).</i></p>	<p>10. § (2) bekezdés <i>A munkáltató a munkavállalóra vonatkozó (...) adatot (...) harmadik személlyel csak törvényben meghatározott esetben vagy a munkavállaló hozzájárulásával közölhet.</i></p>

Ezen rendelkezésekből fakadó gyakorlati követelmények:

- A külföldre történő adattovábbítás alapvető követelményeit a tájékoztató 4. pontja tartalmazza.
- Az Infotv. 3. § 13. pontja értelmében adattovábbításnak minősül az, amikor személyes adatot meghatározott harmadik személy számára hozzáférhetővé tesznek. Az Infotv. 3. § 22. pontja alapján harmadik személy az adatkezelőn, az érintetten és az adatfeldolgozón kívül minden más személy és szervezet. A munkaviszonyban az érintett a munkavállaló, az adatkezelő a munkáltató, és minden, rajtuk kívüli személy harmadik személynek minősül, így például harmadik személynek minősülnek a munkáltatóval egy vállalatcsoportban lévő más vállalatok is. Ebből fakadóan adattovábbításnak tekinthető az is, amikor a munkáltató egy közös adatbázisba tölti fel a munkavállalók személyes adatait, amely adatbázishoz más adatkezelők (más leányvállalatok, az anyavállalat) is hozzáférhet.
- Ugyanez a helyzet a munkáltató tulajdonosát tekintve is: főszabályként a tulajdonosi jogok gyakorlása nem teszi szükségessé, és nem engedi meg a munkavállalókra vonatkozó személyes adatok tulajdonos részére való továbbítását. Kivételt ez alól csupán a vezető állású munkavállalók jelenthetnek, egyéb esetben azonban a tulajdonos részére csak személyazonosításra alkalmatlan adatok továbbíthatóak.
- Az Mt. rendelkezéséből következik az is, hogy egy álláspályázatra jelentkezéskor az állást meghirdető munkáltató nem jogosult a korábbi munkáltatótól információkat gyűjteni, és ily módon „leinformálni” a pályázót. Ebben az esetben a korábbi munkáltató semmilyen személyes adatot nem közölhet az állást meghirdető munkáltatóval, hiszen – törvényi felhatalmazás hiányában – az Mt. 10. § (2) bekezdése csak a munkavállaló hozzájárulásával tehetné ezt meg.

3. Az előzetes tájékoztatás követelménye

Infotv.	Mt.
<p>20. § (1)-(2) bekezdés <i>Az érintettel az adatkezelés megkezdése előtt közölni kell, hogy az adatkezelés hozzájáruláson alapul vagy kötelező. Az érintettet az adatkezelés megkezdése előtt egyértelműen és részletesen tájékoztatni kell az adatai kezelésével kapcsolatos minden tényről, így különösen az adatkezelés céljáról és jogalapjáról, az adatkezelésre és az adatfeldolgozásra jogosult személyéről, az adatkezelés időtartamáról, arról, ha az érintett személyes adatait az adatkezelő a 6. § (5) bekezdése alapján kezeli, illetve arról, hogy kik ismerhetik meg az adatokat. A tájékoztatásnak ki kell terjednie az érintett adatkezeléssel kapcsolatos jogaira és jogorvoslati lehetőségeire is.</i></p>	<p>9. § (2) bekezdés <i>A személyiségi jog korlátozásának módjáról, feltételeiről és várható tartamáról a munkavállalót előzetesen tájékoztatni kell.</i></p> <p>10. § (2) bekezdés <i>A munkáltató köteles a munkavállalót tájékoztatni személyes adatainak kezeléséről.</i></p> <p>11. § (2) bekezdés <i>A munkáltató előzetesen tájékoztatja a munkavállalót azoknak a technikai eszközöknek az alkalmazásáról, amelyek a munkavállaló ellenőrzésére szolgálnak.</i></p>

Ezen rendelkezésekből fakadó gyakorlati követelmények:

- Az érintett az előzetes, megfelelő tájékoztatás alapján képes felismerni azt, hogy az adott adatkezelés milyen hatással van az információs önrendelkezési jogára és a magánszférájára.
- Az előzetes tájékoztatásra vonatkozó követelményeket a jogalkotó az Infotv. 20. §-ában fogalmazta meg. Az előzetes, megfelelő tájékoztatás kötelezettségének központi eleme az Infotv. 20. § (2) bekezdése, amely felsorolja azokat az alapvető adatkezelési körülményeket, amelyekről az adatkezelőnek tájékoztatást kell nyújtania. Az előzetes tájékoztatás adatvédelmi követelményeiről szóló ajánlás¹⁴ részletesen foglalkozik az előzetes tájékoztatási kötelezettséggel.
- Amennyiben a munkáltató technikai eszközzel kíván ellenőrzést végezni – tekintve, hogy az ellenőrzés személyes adatok kezelésével jár együtt – úgy az nem lehet titkos, arról a munkavállalókat előzetesen tájékoztatni kell, így például a munkavállalóknak tisztában kell lenniük az ellenőrzés módjával, céljával.
- A munkahelyi adatkezelésekkel összefüggésben kiemelten fontos arról tájékoztatást nyújtani, hogy a munkáltató szervezetrendszerén belül ki férhet hozzá a személyes adatokhoz. Azt a személyi kört, akik hozzáférhetnek a személyes adatokhoz, adatkezelési célonként külön-külön kell meghatározni.

¹⁴ Az ajánlás pontos elérhetősége megtalálható a tájékoztató IV. pontjában.

4. Adattovábbítás külföldre

A Hatósághoz gyakran fordulnak több országban is képvisellel rendelkező, multinacionális társaságok azzal a kérdéssel, hogy van-e lehetőség a cégen belül munkavállalók személyes adatainak továbbítására, és amennyiben igen, milyen szabályok is vonatkoznak az adattovábbításra. A kérdés megválaszolásához az Mt. és az Infotv. nyújt segítséget.

4.1. Adattovábbítás az EGT-n belül

Az Infotv. 8. § (4) bekezdése szerint az EGT-államba irányuló adattovábbítást úgy kell tekinteni, mintha Magyarország területén belüli adattovábbításra kerülne sor. Az Infotv. rendelkezése természetesen irányadó a munkáltatók adattovábbításaira is, azokkal a korlátozásokkal, amelyeket az Mt. tartalmaz.

Az Mt. 10. § (2) bekezdés alapján a munkáltató a munkavállalóra vonatkozó adatot harmadik személlyel csak törvényben meghatározott esetben vagy a munkavállaló hozzájárulásával közölhet. Ennek megfelelően tehát az általános szabályok az irányadóak, figyelembe véve a jogalapoknál kifejtetteket, vagyis, hogy az érintett hozzájárulása a munkavégzésre irányuló jogviszonyokban az önkéntessége miatt nehezen értelmezhető, ezért az adattovábbítás során más jogalapok alkalmazása lehet indokolt.

4.2. Adattovábbítás az EGT-n kívülre

Amennyiben nem EGT-államban, azaz harmadik országban honos adatkezelő vagy adatfeldolgozó részére történik az adatok továbbítása, akkor arra elsődlegesen az Infotv. 8. § (1)-(2) bekezdésében megjelölt esetekben kerülhet sor.

Ez alapján – a munkahelyi adatkezelések sajátosságaira is figyelemmel – két esetkör alapján lehet harmadik országban honos munkáltató (adatkezelő, adatfeldolgozó) számára adatot továbbítani:

1. Az első esetkör az érintett kifejezett hozzájárulásán alapuló adattovábbítás. Mint már szó volt róla a tájékoztató 3.1. pontjában, ezen jogalap esetében figyelemmel kell lenni arra, hogy a hozzájárulás mint az adatkezelés vagy az adattovábbítás jogalapja, kivételesen alkalmazható csak. A munkáltatótól elvárható, hogy a munkavállalók személyes adatait csak megfelelő védelmet nyújtó harmadik országokba továbbítsa, vagy az Infotv. és az uniós jogszabályok által rögzített más módon biztosítsa a megfelelő szintű védelmet az adattovábbítással összefüggésben.
2. A második esetkör az érintett kifejezett hozzájárulásának hiányában, ha az alábbi konjunktív feltételek teljesülnek:
 - a. az Infotv. hatálya alá tartozó adatkezelő (az adattovábbító szervezet) az Infotv. vagy az Adatvédelmi Irányelv által elismert jogalappal rendelkezik az adatkezeléshez, és
 - b. a harmadik országban a személyes adatok megfelelő szintű védelme biztosított, mivel:
 - i. az adattovábbítással összefüggésben az Európai Unió kötelező erejű jogi aktust fogadott el, vagy
 - ii. az adattovábbításra vonatkozó kötelező szervezeti szabályozást (angol nyelvű elnevezéssel: *binding corporate rules*; a továbbiakban: BCR) a Hatóság jóváhagyta. A BCR lehetővé teszi, hogy egy multinacionális vállalat Infotv. hatálya

alá tartozó tagja személyes adatokat továbbítson az EGT-térségen kívüli országokban található tagjai részére oly módon, hogy az adattovábbítás megfeleljen mind az uniós, mind a magyar adatvédelmi követelményeknek.¹⁵

Az Infotv. 8. § (2) bekezdés a) pontja szerinti uniós kötelező erejű jogi aktusok köre tovább bővült. Az Európai Bizottság 2016. július 12-én ugyanis elfogadta az EU-USA adatvédelmi pajzsot (Privacy Shield határozat). Ez az új keretrendszer védelmezi minden olyan uniós polgár alapvető jogait, akinek a személyes adatait az Egyesült Államokba továbbították, valamint egyértelmű jogi helyzetet teremt azoknak a vállalkozásoknak a számára, amelyek igénybe veszik az Egyesült Államokba irányuló adattovábbításokat. A Privacy Shield határozat – melynek jelenleg felülvizsgálata zajlik – az Európai Unió kötelező erejű jogi aktusának tekinthető, ezért megfelelő szintű védelmet biztosíthat a külföldi adattovábbítások esetén.

5. Az adatvédelmi nyilvántartásba való bejelentési kötelezettség

Az Infotv. 65. § (3) bekezdés a) pontja szerint nem vezet adatvédelmi nyilvántartást a Hatóság arról az adatkezelésről, amely az adatkezelővel munkaviszonyban álló személyek adataira vonatkozik. Ez a kivétel vonatkozik minden munkaviszony jellegű egyéb jogviszonyra is. A nyilvántartásba vétel alóli felmentés kiterjed a munkáltató teljes adatkezelésére, tehát az általa folytatott adatkezelésekről a Hatóság nem vezet nyilvántartást. Kizárólag azokat az adatkezeléseket nem kell bejelenteni a nyilvántartásba, amelyeket a munkáltató számára a jogszabályok kötelezően előírnak. Ezeknek az adatkezeléseknek (például a társadalombiztosítással, a személyi jövedelemadózással kapcsolatban az illetékes szervek felé történő adattovábbítások) a célja a munkavállalók számára is ismert, ezért nem szükséges a bejelentés. Kiemelendő, hogy a munkáltató által végzett, jogszabályban előírt adatkezeléssel kapcsolatos nyilvántartásokat (például közszolgálati nyilvántartás, a munkáltató keretein belül folytatott bérszámfejtés kapcsán létrejött adatbázis), illetve a munkavállalók ellenőrzésével kapcsolatos adatkezeléseket sem kell bejelenteni az adatvédelmi nyilvántartásba. A bejelentés alóli mentességnek az ad alapot, hogy a személyes adatok kezelése az érintettel fennálló jogviszonyhoz kötődik. Abban az esetben, ha az adatkezelés célja eltér a jogszabályokban a munkáltató számára előírt adatkezelési céloktól, nem állnak fenn a mentesség feltételei.

Mindezek mellett az Infotv. 65. § (3) bekezdés d) pontja szerint a Hatóság arról az adatkezelésről sem vezet nyilvántartást, mely az érintett anyagi és egyéb szociális támogatása céljából nyilvántartott személyes adataira vonatkozik. Ezt a kivételt a Hatóság széles körben értelmezi, kiterjed minden jogszabályban szabályozott anyagi és szociális támogatás nyújtásával kapcsolatos adatkezelésre, legyen az például a munkáltatón keresztül igénybe venni kívánt adókedvezmény, támogatás, melyhez adott esetben a munkavállalók hozzátartozóinak személyes adataira is szükség van.

A kamerarendszerrel összefüggő adatkezelések esetében tekintettel kell lenni arra, hogy az adott helyiségben kik tartózkodhatnak, hiszen bizonyos helyiségek esetében a megfigyelték nem csak munkavállalók lehetnek, hanem más, az elektronikus vagyónvédelmi rendszer által megfigyelt területen tartózkodó személyek is (így például ügyfelek, látogatók). Amennyiben a munkahelyen

¹⁵ A Hatóság a honlapján a „Kötelező szervezeti szabályozás (BCR)” menüpont alatt további információk találhatóak a BCR-rel összefüggésben: <http://naih.hu/mit-jelent-a-koetelez--szervezeti-szabalyozas--bcr--.html>

alkalmazott elektronikus megfigyelőrendszer érintetti köre túlmutat az Infotv. 65. § (3) bekezdés a) pontján, azaz nem csak a munkavállalók kerülhetnek a kamerák látókörébe, akkor az adatkezelést be kell jelenteni az adatvédelmi nyilvántartásba. Ellenkező esetben az adatkezelés a kivételszabály alá esik, és ennek megfelelően bejelentési kötelezettség sem terheli a munkáltatót.

Az állaspályáztatásokkal összefüggő adatkezelések esetében munkaviszonyról még nem beszélhetünk, ezért a fenti kivételszabály nem alkalmazható. Helyette azonban szintén mentesülést jelenthet a nyilvántartásba vételi kötelezettség alól, ha az adatkezelés megfelel a szintén az Infotv. 65. § (3) bekezdés a) pontja szerinti ügyfélkapcsolat feltételeinek.

Az ügyfélkapcsolat fogalmát az Infotv. nem definiálja, a Hatóság gyakorlata szerint az alábbi követelményeknek kell megfelelnie az adatkezelésnek, hogy ügyfélkapcsolatról lehessen beszélni:

- az adatokat közvetlenül az érintettektől veszik fel,
- az adatkezelés célja az érintettek számára ismert,
- a kezelendő adatok fajtája, az adatkezelés időtartama (adattörlés) előre meghatározott,
- az adatokat csak az előre meghatározott céllal összefüggésben használják fel,
- az adatok nem kerülnek ki az adatkezelő kezeléséből,
- az érintetteket minderről megfelelően tájékoztatják.

Amennyiben az állaspályáztatással összefüggő adatkezelés megfelel ezen ügyfélkapcsolat szempontjából releváns kritériumoknak, az adatkezelést az adatvédelmi nyilvántartásba nem kell bejelenteni, ellenkező esetben bejelentési kötelezettség áll fenn.

A munkáltatói belső visszaélés-bejelentési rendszert a Pktv. rendelkezése¹⁶ alapján kell bejelenteni az adatvédelmi nyilvántartásba.

6. A munkahelyi adatkezelésekkel kapcsolatos joghatósági kérdések

A Hatóság tapasztalatai alapján gyakran fordul elő az, hogy az adatkezelési körülményeket nem az Infotv. hatálya alá tartozó adatkezelő, hanem annak EGT-államban¹⁷ vagy harmadik országban¹⁸ található tulajdonosa határozza meg, illetve sok esetben e tulajdonos is végzi az adatkezelést. Erre egy gyakori példa visszaélés-bejelentő rendszerek alkalmazása, amelyeket sokszor úgy alkalmaznak Magyarországon, hogy a már meglévő rendszereket „kiterjesztik” hazánkban található adatkezelőre is.

Az országhatáron átnyúló adatkezelések esetében felmerül az a kérdés, hogy alkalmazni kell-e a magyar jogszabályokat abban az esetben, amikor az adatkezelő tulajdonosa az adatkezelés mindennapi gyakorlatának kialakítása során más EGT-állam jogszabályait vette alapul.

E kérdésben elsődlegesen az Adatvédelmi Irányelv 4. cikk (1) bekezdés a) alpontja irányadó. Eszerint a nemzeti rendelkezések alkalmazandóak, ha az adatkezelést „a tagállam területén az adatkezelő egy szervezete tevékenységeinek keretében végzi; amennyiben ugyanaz az adatkezelő több tagállam területén is letelepedett, meg kell tennie a szükséges intézkedéseket

¹⁶ Pktv. 14. § (1) bekezdés

¹⁷ Az Infotv. 3. § 23. pontja

¹⁸ Az Infotv. 3. § 24. pontja

annak biztosítása érdekében, hogy szervezeteinek mindegyike megfeleljen az alkalmazandó nemzeti jog által megállapított kötelezettségeknek.”

Az Adatvédelmi Irányelv 29. cikke szerint létrehozott Adatvédelmi Munkacsoportnak az alkalmazandó jogról szóló 8/2010. számú véleménye szerint az alkalmazandó jog meghatározása szempontjából az Irányelv fenti rendelkezésében szereplő „*tevékenységeinek keretében*” fordulata rendelkezik döntő jelentőséggel, és nem pedig az, hogy például a személyes adatokat hol tárolják. E kifejezés nem azt jelenti, hogy az alkalmazandó jog annak a tagállamnak joga, ahol az adatkezelő letelepedett, hanem ahol az adatkezelő egy szervezete az adatkezeléshez vagy az adatfeldolgozáshoz kapcsolódó tevékenységekben részt vesz. Tehát kiemelt szerepe van az egyes szervezetek részvételének azokban a tevékenységekben, amelyek keretében az adatkezelést végzik. Ha egy szervezet saját tevékenységei keretében kezel vagy dolgoz fel személyes adatokat, az alkalmazandó jog azon tagállam joga lesz, ahol e szervezet található. Ha a szervezet egy másik szervezet tevékenységei keretében kezel vagy dolgoz fel személyes adatokat, az alkalmazandó jog azon tagállam joga lesz, ahol a másik szervezet található.

Az alkalmazandó jog meghatározására irányadó szabályokkal az Európai Unió Bírósága is foglalkozott a Google spanyolországi leányvállalatának tevékenységével kapcsolatban hozott ítéletében.¹⁹ A Bíróság megállapította, hogy a Google szolgáltatáshoz „*hasonló, harmadik államban letelepedett, azonban a tagállamok egyikében szervezettel rendelkező vállalkozás által működtetett keresőmotort kiszolgáló személyesadat-kezelés [helyesen: adatkezelés] e szervezet „tevékenységeinek keretében” végzett adatkezelésnek minősül, ha a szervezetet arra hozták létre, hogy ebben a tagállamban biztosítsa az e keresőmotor által kínált reklámhelyek értékesítését és reklámozását, amelyek a keresőmotor által nyújtott szolgáltatás nyereségességét szolgálják.*” A Google Inc.-nek mint a keresőmotor működtetőjének, illetve az adott tagállamban található leányvállalatának tevékenységei elválaszthatatlanul összekapcsolódnak, mivel a reklámhelyekkel kapcsolatos tevékenységek jelentik azt az eszközt, amelyek a szóban forgó keresőmotort nyereségessé teszik, és ugyanakkor ez a keresőmotor teszi lehetővé e tevékenységek végzését. Erre alapozva a testület végül megállapította, hogy „*a személyes adatok kezelését e rendelkezés értelmében a tagállam területén az adatkezelő egy szervezete tevékenységeinek keretében végzik, ha a keresőmotor működtetője az egyik tagállamban olyan irodát nyit vagy leányvállalatot hoz létre a keresőmotor által kínált reklámhelyek értékesítésére és reklámozására, amelynek tevékenysége az adott állam lakosai felé irányul.*”

Ennek megfelelően, ha az Infotv. alá tartozó adatkezelő Európai Unióban vagy harmadik országban található tulajdonosának tevékenységével megegyező, vagy ahhoz kapcsolódó tevékenységet végez, és ezzel a tevékenységgel összefüggésben kerül sor a munkahelyi adatkezelésre, akkor az Adatvédelmi Irányelv 4. cikk (1) bekezdés a) pontja vonatkozásában úgy kell tekinteni, mintha az adatkezelést a „*tevékenységeinek keretében*” végeznék, és alkalmazni kell a magyar jogszabályokat. A Hatóság álláspontja szerint a joghatóság kérdésében különös figyelemmel kell lenni továbbá arra a körülményre is, hogy a hazánkban végzett munkahelyi adatkezelések alapján alapvetően Magyarországon alkalmazzák a jogkövetkezményeket, vagyis az adatkezelés egyik fontos eleme, az érintettre vonatkozó következtetés levonása és a személyes adat felhasználása szintén Magyarország területén történik. Ez is azt támasztja alá, hogy ezekben az esetekben alkalmazni kell a magyar jogszabályi rendelkezéseket is.

¹⁹ A tájékoztató IV. pontjában megtalálható az Európai Unió Bírósága döntésének pontos megnevezése és elérhetősége.

Mindezek alapján, a jelen tájékoztatóban kifejtett adatvédelmi követelményeket alkalmazni kell abban az esetben is, ha a munkahelyi adatkezelés szabályait az EGT-állam vagy harmadik ország jogszabályai alapján határozták meg, de ezen adatkezeléseket Magyarországon is végzik akár az Infotv. hatálya alá tartozó, akár más ország joga szerint létrejött adatkezelők.

II. Egyes speciális munkahelyi adatkezelések

1. Az álláspályázatra jelentkezés és a magán-munkaközvetítés

1.1. „Anonim álláshirdetések”

Anonim álláshirdetések alatt azok az álláshirdetések értendők, amelyekben a munkáltató nem tünteti fel a cégnevet, ezért az álláspályázat elküldésének időpontjában a jelentkezők nem lehetnek tisztában azzal, hogy mely munkáltatónak az állására jelentkeznek.

A Hatóság gyakorlata szerint az álláshirdetésre jelentkezők információs önrendelkezési jogának szerves része az, hogy az érintettek az adatkezelő kilétére kiterjedő megfelelő tájékoztatást kapjanak már az adatkezeléshez való hozzájárulás megadása előtt, valamint hogy tudomással rendelkezzenek arról, hogy kikkel szemben tudnak élni az Infotv.-ben szereplő jogaikkal. Bizonyos esetekben ezzel szemben állnak a munkáltató gazdasági vagy egyéb érdekei, hogy kiléte rejtve maradjon a pályázat során mindaddig, amíg ez indokolt (például egy cég nem szeretné, ha idő előtt kiderülne, hogy „belép a piacra”, ezt szeretné a konkurencia előtt titokban tartani). Ebben a gyakorlatban rendkívül egyenlőtlen helyzetben vannak a felek, hiszen míg az érintettek jelentkezésük elküldésével azonnal „kiadják magukat”, minden személyes adatukat megismeri az álláshirdetést feladó munkáltató, addig a munkáltató egyáltalán nem ad semmilyen tájékoztatást a személyéről, ezáltal is fokozva a munkavállalók kiszolgáltatottságát, és a munkáltató információs fölényét.

Alapvetően nem fogadható el a munkáltatók részéről az anonim álláshirdetések feladása, mivel az esetek túlnyomó többségében ezzel aránytalanul sérül a jelentkezők információs önrendelkezési joga, így különösen az a joga, hogy a jelentkezők az adatkezelés megkezdése előtt (a pályázati anyag elküldése előtt) valamennyi lényeges adatkezelési körülményéről tájékoztatást kapjanak. A munkáltatók érdekei csak különösen indokolt, rendkívüli esetben, és akkor is legfeljebb korlátozott mértékben (például egy rövid, átmeneti időtartamig) írhatják felül a jelentkezők információs önrendelkezési jogát.

A Hatóság emellett az álláshirdetéseket kínáló honlapok adatkezelésével kapcsolatban is több követelményt állapított meg egy 2015-ös határozatában²⁰, amelyekkel biztosítható a megfelelő egyensúly az érintettek információs önrendelkezési joga és a munkáltatói érdekek között.

1.2. Az álláspályázatra jelentkező munkavállaló valamely közösségi oldalon létrehozott profiljának megtekintése

Egy munkáltató igyekszik a lehető legtöbbet megtudni az álláshirdetésre jelentkezőkről, minden lehetséges forrásból szeretne információt gyűjteni róluk, hogy azok alapján közülük a legmegfelelőbb személyt válassza ki. Ennek egyik kézenfekvő megoldása az, ha a munkáltató megnézi a jelentkezőnek a közösségi oldalon található profiloldalát.

²⁰ NAIH-1159-15/2015/H. számú határozat. Ezzel kapcsolatban azonban szükséges megjegyezni, hogy a határozat bírósági felülvizsgálata folyamatban van. A határozat elérhetősége megtalálható a tájékoztató IV. pontjában.

A közösségi oldalakon mindenki maga állítja be, hogy az általa megosztott tartalmat ki láthatja, ki férhet hozzá. Az érintett kontroll alatt tudja tartani azt, hogy milyen, mindenki számára nyilvános információk érhetőek el róla a közösségi oldalon keresztül. A Hatóság álláspontja szerint továbbá életszerűtlen elvárni a munkáltató oldaláról, hogy ne tekinthesse meg azokat a bárki számára elérhető, nyilvános információkat, amelyeket az álláshirdetésre jelentkező személy osztott meg magáról.

A közösségi oldalak megtekintésével összefüggésben azonban a munkáltatónak az alábbi adatvédelmi követelményekre kell tekintettel lennie:

- Előzetes tájékoztatást kell biztosítani a jelentkezők számára. Így például ismertetni kell a jelentkezőkkel, hogy a felvételi eljárás folyamata kiterjed arra is, hogy a munkáltató is megtekinti a jelentkező közösségi oldalon létrehozott, bárki számára nyilvános információit. Azaz a munkáltató nem „rejtetheti el” ezen gyakorlatát a jelentkezők előtt, fel kell fednie a kiválasztási folyamat minden lényeges részét.
- Nem fogadható el az, ha a munkáltató a korlátozottan nyilvános adatokat ismeri meg. Ilyen például az az eset, amikor az álláshirdetésre jelentkező személy tagja valamely zárt csoportnak egy közösségi oldalon belül, és ennek ismeretében a munkáltató megkér valakit, aki szintén tagja ennek a zárt csoportnak, hogy nézze meg, mit is csinál a jelentkező ezen személy a zárt csoporton belül. Ezen információk már nem teljesen nyilvánosak, ezért ezek megismerése már korlátozza a jelentkező magánszférájához való jogát.
- Fontos továbbá az is, hogy – az Mt. 10. § (1) bekezdésében foglaltakkal összhangban – csak azok az információk ismerhetők meg, amelyek lényegesek az álláspályázattal vagy a munkakörrel kapcsolatban. A munkaviszony létesítése szempontjából így például nem lényeges adat a magánéletre, párkapcsolatra, családi életre, vallásra vonatkozó adat.
- Az érintett közösségi oldalon végzett, nyilvános tevékenysége megismerhető, következtetést vonható le arról, de a további adatkezelési műveletek már jogellenesnek minősülnek. Vagyis arra nincs lehetőség, hogy a jelentkező profiloldalát a munkáltató lementse, tárolja vagy más számára továbbítsa.

1.3. A pályázatok, önéletrajzok megőrzése

Az Infotv. 4. § (1)-(2) bekezdése alapján az önéletrajzok, pályázatok esetében az adatkezelés célja az, hogy a meghirdetett munkakört betöltsék. Ennek megfelelően, ha a munkáltató a jelentkezők közül kiválasztott egy személyt a meghirdetett állásra, akkor megszűnt az adatkezelés célja, és – az Infotv. 17. § (2) bekezdés d) pontja²¹ alapján – a ki nem választott jelentkezők személyes adatait törölni kell. Ezzel egyidejűleg fennáll a törlési kötelezettség abban az esetben is, ha az érintett még a jelentkezés során meggondolja magát, visszavonja pályázatát.

²¹ Az Infotv. 17. § (2) bekezdés d) pontja értelmében: „a személyes adatot törölni kell, ha (...) az adatkezelés célja megszűnt (...)”

Emellett a pályázati anyagok kezelésével kapcsolatban figyelembe kell venni a speciális jogszabályi rendelkezéseket is.²²

A munkáltató alapvetően csak az érintett kifejezett, egyértelmű és önkéntes hozzájárulása alapján őrizheti meg a pályázatokat, feltéve, ha azok megőrzésére az Infotv. 4. § (1)-(2) bekezdésével összhangban álló adatkezelési célja elérése érdekében szükség van. A Hatóság ezzel kapcsolatban kiemeli, hogy ha az érintett elküldi a pályázati anyagát a munkáltató számára, akkor ez jelenti azt, hogy hozzá is járul ahhoz, hogy a pályázati anyagát a munkáltató megőrizze, mivel ebben az esetben megkérdőjelezhető a munkavállaló hozzájárulásának önkéntessége. Erre tekintettel a Hatóság álláspontja szerint az a jó gyakorlat a munkáltató részéről, ha a hozzájárulást a felvételi eljárás lezárását követően kéri a jelentkezőktől. Emellett a munkáltatónak a pályázati anyagok megőrzése esetében is egy konkrét, az adatkezelés céljához és az adatkezelés pontosságának, naprakészségének elvéhez igazodó időtartamot kell meghatározni.

1.4. A pályázati anyagok kezelésével kapcsolatos egyéb adatvédelmi követelmények

A jelentkezők információs önrendelkezési jogát az biztosítja a legmagasabb szinten, ha tájékoztatást kapnak arról is, ha a munkáltató nem őt választotta az adott állásra. Ennek megfelelően a munkáltató részéről nem fogadható el az a gyakorlat, ha például az álláshirdetésben kiköti, hogy amennyiben az adott jelentkező nem kap külön értesítést, akkor a munkáltató nem vette fel a jelentkezőt az adott állásra.

Az Infotv. szabályozása alapján személyes adatnak minősül az adatból levont, az érintettre vonatkozó következtetés is. Ennek megfelelően, ha a munkáltató bármilyen feljegyzést készít a pályázóról, akkor az is a pályázó személyes adatának minősül. Ezzel kapcsolatban két adatvédelmi követelményt szükséges tisztázni:

- Egyrészt erre is kiterjed az érintettet tájékoztatáshoz való joga, vagyis, hogy megismerje, a munkáltató milyen következtetéseket vont le a pályázati anyagával összefüggésben.
- Másrészt a munkáltatónak törölnie kell az ilyen természetű, az érintettre levont következtetéseket tartalmazó feljegyzéseket is.

1.5. A magán-munkaközvetítő által kezelhető adatok

A 118/2001. (VI. 30.) Korm. rendelet 10. § (1) bekezdés e) pontja meghatározza, hogy milyen adatokat nem lehet kezelni magán-munkaközvetítés során. A jogszabály értelmében tilos olyan személyes adatokat kezelni, amelyekre a munkát keresők alkalmasságának a megítéléséhez nincs szükség, illetve amelyek a keresett munkával nincsenek közvetlen összefüggésben.

Erre tekintettel a magán-munkaközvetítő a képesítésre, szakmai tapasztalatra vonatkozó adatokat és az alkalmasság megítéléséhez szükséges adatokat kezelheti.

²² Így például a Kjt. 20/A. § (7) bekezdése alapján „sikertelen pályázat esetén a pályázó részére a pályázati anyagot vissza kell juttatni. Amennyiben a pályázó az általa benyújtott, személyes adatokat tartalmazó adathordozót a pályázat elbírálási határidejétől számított kilencven napon belül nem veszi át, azokat meg kell semmisíteni és személyes adatait törölni kell.”

Ha a munkát kereső munkavállaló azt tapasztalja, hogy a magán-munkaközvetítő mégis olyan adatot kér tőle, amely adat kezelésének célja nem egyértelmű, akkor az érintett magyarázatot, tájékoztatást kérhet a magán-munkaközvetítőtől.

2. Alkalmassági vizsgálatok

2.1. Általános adatvédelmi követelmények

Az Mt. 10. § (1) bekezdése²³ alapján a munkavállalókkal szemben kizárólag két típusú alkalmassági vizsgálat alkalmazható:

- Egyrészt vannak olyan alkalmassági vizsgálatok, amelyeket munkaviszonyra vonatkozó szabály ír elő.
- Másrészt vannak olyanok is, amelyeket nem ír ugyan elő munkaviszonyra vonatkozó szabály, de amelyre a munkaviszonyra vonatkozó szabályban meghatározott jog gyakorlása, kötelezettség teljesítése érdekében szükség van.

Az alábbi adatvédelmi követelmények az alkalmassági vizsgált mindkét esetkörülményre egyaránt vonatkoznak:

- Részletesen tájékoztatni kell a munkavállalókat többek között arról, hogy az alkalmassági vizsgálat milyen készség, képesség felmérésére irányul, a vizsgálat milyen eszközzel, módszerrel történik. Amennyiben jogszabály írja elő a vizsgálat elvégzését, akkor tájékoztatni kell a munkavállalókat a jogszabály címéről és a pontos jogszabályhelyről is.
- A vizsgált munkavállalók, illetve a vizsgálatot végző szakember ismerhetik meg az eredményeket. Ezt azért is fontos hangsúlyozni, mert a tesztből akár olyan következtetés is levonható, amely maga az érintettek, a munkavállalók számára sem volt ismert. A munkáltató csak azt az információt kaphatja meg, hogy a vizsgált személy a munkára alkalmas-e vagy sem, illetve milyen feltételek biztosítandók ehhez. A vizsgálat részleteit, illetve annak teljes dokumentációját azonban nem ismerheti meg.

2.2. A munkáltató által előírt alkalmassági vizsgálatok követelményei

Ebben az esetben a munkáltatónak el kell végeznie a már korábban ismertetett érdekmérlegelési tesztet, hiszen az alkalmassági vizsgálatok elvégzésével együtt járó adatkezelés esetében is az adatkezelés jogalapja a munkáltató jogos érdeke lehet. Az érdekmérlegelési teszt során a munkáltatónak számos szempontra kell figyelemmel lennie. Így például a munkáltató által választott módszernek alkalmasnak kell lennie a cél elérésére, a munkaviszonnyal kapcsolatos, releváns adatot kell a teszteredményből kapni. Másfelől az alkalmassági vizsgálat szükségességét a munkáltatónak meg kell indokolnia. Az adatkezelésnek természetesen célhoz kötöttnek kell

²³ Az Mt. 10. § (1) bekezdése kimondja, hogy „munkavállalóval szemben csak olyan alkalmassági vizsgálat alkalmazható, amelyet munkaviszonyra vonatkozó szabály ír elő, vagy amely munkaviszonyra vonatkozó szabályban meghatározott jog gyakorlása, kötelezettség teljesítése érdekében szükséges.”

lennie, azaz csak akkor lehet jogszerű, ha annak a vizsgálatnak az elvégzése szükséges a munkaviszony létesítése, fenntartása szempontjából.

Ezen túlmenően az alkalmassági vizsgálatokkal kapcsolatban a munkáltatónak további sajátosságokra kell figyelemmel lennie. Így példaként említhető a munkáltatók által gyakran alkalmazott, a különböző kompetenciák, személyiségjegyek felmérésére alkalmas tesztek kitöltetése. A tesztek eredménye azonban túlmutathat az alkalmasság megítélésén, és a munkavállalók személyes – és bizonyos esetekben különleges – adataira világít rá. A tesztek két fő típusát lehet elhatárolni: léteznek munkaalkalmasságra, felkészültségre irányuló tesztlapok, illetve pszichológiai vagy személyiségjegyeket kutató tesztlapok. Az előbbieket a munkáltató mind a munkaviszony létesítése előtt, mind pedig a munkaviszony fennállása alatt kitöltetheti a munkavállalókkal. Más megítélés alá esnek a pszichológiai vagy személyiségjegyeket kutató tesztlapok. Az egyértelműen munkaviszonnyal kapcsolatos, a munkafolyamatok hatékonyabb ellátása, megszervezése érdekében kitöltethető a munkavállalók nagyobb csoportjával a személyiségjegyek kutatására alkalmas tesztlap, de csak akkor, ha az elemzés során felszínre került adatok nem köthetők az egyes konkrét munkavállalókhöz, vagyis anonim módon történik az adatok feldolgozása.

2.3. A munkaviszony fennállta alatt végzett munkahelyi tréningek adatvédelmi követelményei

Általában a tréningek, különböző alkalmassági vizsgálatok keretén belül elvégzett tesztek komoly személyiségjellemzést adnak a munkavállalókról, amelyek megismerése, tárolása, nyilvántartása nem fogadható el a munkáltatók részéről. A tesztek kitöltése a trénernek (szakembernek) ad iránymutatást a tréningen résztvevő munkavállalókról: kinek milyen képességét szükséges fejleszteni, milyen módszerrel lehet eredményesebb munkavégzést elérni. Azaz a teszteredményeket a szakértő kezeli a tréning során, és ennek átadása a munkáltató részére nem elfogadható. Továbbá a tréninget követően a tréner vagy a trénercég arra alapvetően nem jogosult, hogy egy tréningen résztvevő személy eredményeit névhez köthetően a jövőben is kezelje, ehelyett javasolt a kitöltött tesztlapok, dokumentumok kitöltő részére való átadása.

3. A munkavállalók feddhetetlen előéletének igazolása

Egyes panaszbeadványok szerint a munkáltatók a munkavállalók feddhetetlen előéletének igazolását hatósági erkölcsi bizonyítvánnyal vagy a bűnügyi nyilvántartásból, az érintett kérelmére kiállított tájékoztatás benyújtásával kérik igazolni.

A hatósági erkölcsi bizonyítvány mint jogintézmény célja többek között az, hogy a munkavállaló a munkáltató előtt erkölcsi alkalmasságát az adott munkakörrel kapcsolatosan igazolja. Erre az érintettet a munkaviszony létesítése előtt, a felvételi eljárás során, illetőleg a munkaviszony fennállása alatt is felszólíthatja a munkáltató, amennyiben az erkölcsi alkalmasság igazolása valamely ágazati jogszabályban meghatározottak szerint, az adott munkakör betöltéséhez valóban elengedhetetlen. Ilyen, jogszabály által előírt adatkezelés található például az Mt. 44/A. §-ában, amelynek alapján nem létesíthető munkajogviszony azzal a személlyel, akivel szemben az Mt. 44/A. §-ában szereplő kizáró feltételek fennállnak.

A Bnyt., illetve a vonatkozó törvények rendelkezései értelmében a hatósági erkölcsi bizonyítvány közokirat, melynek tartalmát mindenki – a munkáltató is – köteles a kiállításától számított kilencven

napig²⁴ valósnak elfogadni. A munkavállalók egyes munkaviszonyokra való erkölcsi alkalmasságát tehát ezen okirat megkérésével lehet igazolni.

Számos esetben a munkáltatók arra kérik a munkavállalókat, hogy a hatósági erkölcsi bizonyítvány helyett a bűnügyi nyilvántartó szervtől igényeljék a bűnügyi nyilvántartási rendszerben kezelt adataikra vonatkozó tájékoztatást.

Jóllehet, a Bnyt. lehetővé teszi azt, hogy az érintett személy a bűnügyi nyilvántartásban szereplő személyes adatairól tájékoztatást kérjen²⁵, ennek célja azonban az, hogy az érintett átláthassa személyes adatainak kezelését és nem az, hogy az érintett személyt – a büntetett előélet alóli mentesüléstől függetlenül – ilyen formán beszerzett adatokkal a munkáltató átvilágítsa.

Azon munkáltatói szándék, miszerint a munkavállaló erkölcsi alkalmasságát az érintett kérelmére a bűnügyi nyilvántartási rendszerben kezelt adatairól kiállított tájékoztatással kívánja megállapítani, súlyosan sérti az érintett személyes adatai védelméhez való jogát, jogellenesen diszkriminálhatja és ellentétes a hátrányos jogkövetkezmények alóli mentesüléshez fűződő közérdekkel.

A munkáltatók azon gyakorlatát, hogy a hatósági erkölcsi bizonyítvány helyett a munkavállalótól a bűnügyi nyilvántartási rendszerben kezelt adataira vonatkozó tájékoztatást – annak díj- és illetékmentes kiállítása miatt – is elfogadják az illetékekről szóló 1990. évi XCIII. törvény 2016. január 1-jét követő módosítása sem indokolja, hiszen a hatályos jogi szabályozás szerint a hatósági erkölcsi bizonyítvány kiállítása iránti eljárás évente négy alkalommal illetékmentes.

4. A munkavállalók munkaviszonnyal összefüggő magatartásának ellenőrzése

4.1. Munkahelyi kamerás megfigyelés

A Hatóság 2013 januárjában egy ajánlást bocsátott ki a munkahelyen alkalmazott elektronikus megfigyelőrendszerekkel összefüggésben²⁶. Az ajánlásban foglaltak továbbra is iránymutatást jelentenek a munkáltatók számára a kamerák alkalmazásával kapcsolatban.

Az alábbi adatvédelmi követelményeket érdemes kiemelni a munkahelyi kamerás megfigyeléssel összefüggésben:

- Külön jogszabály nem rendelkezik a munkahelyen alkalmazott elektronikus megfigyelőrendszerek alkalmazásáról.
- Az Mt. rendelkezései önmagukban nem adnak felhatalmazást a munkáltatónak elektronikus megfigyelőrendszerek alkalmazására, ahhoz a munkáltatónak minden esetben el kell végeznie a jelen tájékoztató jogalapjainál részletesen ismertetett érdekmérlegelési tesztet.
- Kamerákat a munkavállalók és az általuk végzett tevékenység elsődleges, kifejezett megfigyelése céljából működtetni nem lehet. Jogellenesnek tekinthető az olyan

²⁴ Bnyt. 74. § (3) bekezdés

²⁵ Bnyt. 87-88. §

²⁶ A tájékoztató IV. pontjában („Egyéb joganyagok”) megtalálható a Hatóság ajánlásának pontos elérhetősége.

elektronikus megfigyelőrendszer alkalmazása, amelynek – akár nem deklaratív – célja a munkavállalók munkahelyi viselkedésének a befolyásolása.

- Az Mt. mellett az Szvtv. mint mögöttes jogszabály rendelkezéseit is figyelembe kell venni. Az Szvtv. négy esetben teszi lehetővé az elektronikus megfigyelőrendszer alkalmazását:
 - az emberi élet, testi épség, személyi szabadság védelme,
 - a veszélyes anyagok őrzése,
 - az üzleti, fizetési, bank- és értékpapírtitok védelme,
 - vagyonvédelem.²⁷

A célhoz kötött adatkezelés elvéből fakadóan tehát munkahelyen elektronikus megfigyelőrendszert alkalmazni elsődlegesen az Szvtv.-ben elismert ezen célokból lehet, illetve a rögzített felvételek is ezen célokból használhatóak fel. Amennyiben a munkáltatók más célból szeretnék alkalmazni a kamerás megfigyelést, akkor ott igazolniuk kell azt a jogos érdeket, amely – a tájékoztató I. pontjában kifejtettekkel összhangban – szükségessé teszi a kamera alkalmazását.²⁸

- Az elektronikus megfigyelőrendszerek alkalmazhatóságának fontos feltétele, hogy semmiképp sem lehet kamerát elhelyezni olyan helyiségben, amelyben a megfigyelés az emberi méltóságot sértheti, így különösen az öltözőkben, zuhanyzóknak, az illemhelyiségekben vagy például orvosi szobában, váróban.²⁹ Emellett alapvetően szintén nem lehet elektronikus megfigyelőrendszert alkalmazni az olyan helyiségben sem, amely a munkavállalók munkaközi szünetének eltöltése céljából lett kijelölve, mint például a munkavállalók számára biztosított ebédlő. Ez alól kivételt jelenthet az az esetkör, ha ebben a helyiségben valamilyen védendő vagyontárgy található (így például étel-ital automata), amellyel összefüggésben igazolható valamilyen munkáltatói érdek (például a munkavállalók többször megrongálták a berendezést és a károkat a munkáltatónak kellett állnia). Ebben az esetben e konkrét cél érdekében kamera helyezhető el a helyiségben, azonban ekkor a munkáltatónak különös figyelemmel kell lennie arra, hogy a kamera látószöge kizárólag a védendő vagyontárgyra irányulhat.
- A kamerák látószögével kapcsolatban fontos megjegyezni, hogy a munkáltató elektronikus megfigyelőrendszert kizárólag a saját tulajdonában (vagy a használatában) álló épületrészek, helyiségek és területek, illetőleg az ott történt események megfigyelésére alkalmazhat, közterület megfigyelésére azonban nem.
- Az elektronikus megfigyelőrendszer által rögzített felvételek tárolásának időtartamára – más törvényi rendelkezés hiányában – alkalmazni kell az Szvtv. 31. § (2)-(4) bekezdésében szereplő szabályokat. Ennek megfelelően a munkáltató a rögzített felvételeket főszabályként 3 munkanapig tárolhatja, kivéve, ha a megfigyelt helyiséggel kapcsolatban

²⁷ Szvtv. 31. § (1) bekezdés

²⁸ Ezzel kapcsolatban érdemes kiemelni az Adatvédelmi Munkacsoport 6/2014. számú véleményében szereplő példát: „egy vállalat rejtett kamerákat használ arra, hogy azonosítsa az épület dohányzásra nem kijelölt helyeken a dohányzó látogatókat és munkavállalókat. Míg az valóban az adatkezelő jogszerező érdeke, hogy biztosítsa a dohányzás tilalmára vonatkozó jogszabályok betartását, az e célból alkalmazott módszer általában aránytalan és szükségtelenül sérti a magánéletet. Léteznek ennél kevésbé sértő és átláthatóbb módszerek is (például füstérzékelők és látható jelek kihelyezése). Az adatfeldolgozás így nem felel meg a 6. cikkben foglaltaknak, amely előírja, hogy az adatok »gyűjtésük és/vagy további feldolgozásuk célja szempontjából« nem lehetnek »túlzott mértékűek«. Ez a módszer továbbá valószínűleg a 7. cikk szerinti mérlegelési teszten sem felel meg.”

²⁹ Szvtv. 30. § (3) bekezdés

fennállnak az Szvtv. 31. § (3)-(4) bekezdésének feltételei. Ezen túlmenően – a célhoz kötött adatkezelés elvével és az érdekmérlegelés tesztjével összhangban – a munkáltatónak kell igazolni azt, hogyha valamely kamera által rögzített felvételeket három munkanapnál hosszabb időtartamig szükséges megőrizni.

- A munkáltatónak az elektronikus megfigyelőrendszer alkalmazására vonatkozó tájékoztatójában ki kell térnie többek között
 - az adatkezelés jogalapjára, illetve annak sajátosságára (munkáltatói jogos érdeken alapuló adatkezelés),
 - a felvétel tárolásának helyére és időtartamára,
 - a felvételek tárolásával kapcsolatos adatbiztonsági intézkedésekre,
 - az adatok megismerésére jogosult személyek körére, illetőleg arra, hogy a felvételeket mely személyek, szervek részére, milyen esetben továbbíthatja,
 - a felvételek visszanezésére vonatkozó szabályokra, illetőleg arra, hogy a felvételeket milyen célból használhatja fel a munkáltató,
 - arra, hogy a munkavállalókat milyen jogok illetik meg az elektronikus megfigyelőrendszerrel összefüggésben és milyen módon tudják gyakorolni a jogaikat, illetve jogaik megsértése esetén a munkavállalók milyen jogérvényesítési eszközöket vehetnek igénybe.

- A tájékoztatási kötelezettséggel kapcsolatban szükséges kiemelni, hogy a munkáltatónak minden egyes kamera vonatkozásában pontosan meg kell jelölnie, hogy az adott kamerát milyen célból helyezte el az adott területen és milyen területre, berendezésre irányul a kamera látószöge. A munkáltató ezzel igazolni tudja a munkavállalók számára azt, hogy miért tekinthető szükségesnek az adott terület megfigyelése. Nem fogadható el az a gyakorlat, amikor a munkáltató általánosságban tájékoztatja a munkavállalókat arról, hogy elektronikus megfigyelőrendszert alkalmaz a munkahely területén. Tilos továbbá a rejtett kamera használata.

4.2. A munkáltató által a munkavállaló rendelkezésére bocsátott e-mail fiók használatának ellenőrzése

4.2.1. Előzetes intézkedések

Napjainkban a legtöbb munkahelyen a munkáltató „céges e-mail fiókot” bocsát a munkavállalók rendelkezésére (leggyakrabban név@cégnév.hu felépítésű e-mail címetek) annak érdekében, hogy a munkavállalók ezen keresztül tartsák egymással a kapcsolatot, vagy a munkáltató képviseletében levelezzenek az ügyfelekkel, más személyekkel, szervezetekkel.

A „céges e-mail fiók” használatával kapcsolatban gyakori probléma, hogy a levelezőrendszert a munkavállalók saját, személyes céljaikra is használják. Ez visszas helyzetet teremthet abban az esetben, ha a munkáltató – az Mt. 11. §-ában foglalt jogával élve – ellenőrizni kívánja a „céges e-mail fiók” tartalmát és a munkavállalók által folytatott levelezést.

E probléma megelőzéseként a munkáltatónak mindenképp egy belső szabályzatot kell megalkotnia a „céges e-mail fiók” használatának, ellenőrzésének szabályairól. Ezzel ugyanis hatékonyan meg lehet előzni azt, hogy a munkavállalók (és adott esetben más, a magánjellegű levelezésben szereplő érintettek) személyes adatait is kezelje a munkáltató. A belső szabályzatban többek között az alábbiakra szükséges kitérni:

- használható-e magáncélokra a „céges e-mail fiók”,

- az e-mail fiókról biztonsági másolat készítésének és megőrzésének a szabályozására, illetve arra, hogy mikor kerül sor az e-mailek végleges törlésére,
- az e-mail fiók használata ellenőrzésének részletes szabályaira.

Jó gyakorlat lehet a munkáltató részéről továbbá az is, ha bizonyos időközönként emlékezteti a munkavállalókat arra, hogy milyen előírások vonatkoznak a „céges e-mail fiók” használatára (például fél évente a levelezőrendszerben megjelenik egy olyan tájékoztató, hogy a munkavállaló az e-mail fiók használata során magáncélból ne küldjön levelet). Ezzel ugyanis biztosítható az, hogy a munkavállalók kiemelt figyelmet fordítsanak arra, hogy a „céges e-mail fiókot” a munkáltató rendelkezései szerint használják.

A munkáltató megelőző intézkedései ellenére is (például a munkáltató a szabályzatban megtiltja a „céges levelezőrendszer” személyes célú használatát) a munkavállalók sokszor magáncélra is használják az e-mail fiókot. Ebben az esetben – függetlenül attól, hogy a munkáltató egyébként belső szabályzatában megtiltotta az e-mail fiók magáncélú használatát –, a munkáltató a levelezőrendszerben személyes adatokat is kezel, és a munkáltatónak a további intézkedései (például a „céges e-mail fiók” használatának ellenőrzése) során be kell tartania az adatvédelmi követelményeket.

4.2.2. Adatvédelmi követelmények

A „céges e-mail fiók” ellenőrzése esetében a munkáltatói jogos érdek lesz az adatkezelés jogalapja, ezért a munkáltatónak az adatkezelés megkezdése előtt el kell végeznie az érdek mérlegelés tesztjét. Ezen ellenőrzés esetében kiemelt figyelmet kell fordítani az célhoz kötött adatkezelés elvén és a szükségesség-arányosság követelményén túl az érintettek magánszféréjára is, hiszen adott esetben különféle, a munkaviszonyhoz nem kapcsolódó személyes adat is a munkáltató tudomására juthat, illetve vele munkaviszonyban nem álló személyek (az e-mailek küldői vagy címzettjei) adatait is megismerheti.

Ennek megfelelően a munkáltatónak már előzetesen, a szabályzat megalkotása során meg kell határoznia azt, hogy milyen céljai, érdekei miatt kerülhet sor az e-mail fiók ellenőrzésére. Ezen érdekeknek ténylegesnek és valósnak, a munkáltató tevékenységéhez, piaci helyzetéhez és a munkavállalók munkaköréhez igazodóknak kell lenniük. Ezen túlmenően a munkáltatónak az e-mail fiók használatának ellenőrzése előtt közölnie kell a munkavállalókkal, hogy milyen érdeke miatt kerül sor a munkáltatói intézkedésre.

Másrészt a munkáltatónak a fokozatosság elvére figyelemmel lépcsőzetes ellenőrzési rendszert kell kidolgoznia, amelyben megfelelően érvényesülhet a személyes adatok védelme, illetve hogy az ellenőrzés minél kisebb mértékben érintse a munkavállalók magánszféráját.

- 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 cím lesz, és ezért nem szükséges megismerni az e-mail tartalmát. Különösen fontos ez abban az esetben, ha a munkáltató a belső szabályzatban engedélyezi, hogy a munkavállalók a „céges e-mail fiókot” személyes célból is használják, hiszen ekkor a munkavállalók a szabályzattal összhangban magánjellegű leveleket küldhetnek mások számára, vagy fogadhatnak másoktól. 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 nem jogosult megismerni. A kialakult adatvédelmi gyakorlat szerint a munkáltató nem jogosult az e-mail fiókban tárolt magánjellegű e-mailek tartalmát ellenőrizni még akkor sem, ha az ellenőrzés tényéről előzetesen a munkavállalókat tájékoztatta. Az ellenőrzést ekkor a munkavállalók személyes adataik védelméhez való joga, illetve azoknak a nem munkavállaló harmadik személyeknek a személyes adataik védelméhez való joga – továbbá más személyiségi joga, így elsősorban a magántitokhoz és a levéltitokhoz való joga – korlátozza, akik az e-mailt a munkavállalóknak küldték vagy tőlük azt kapták.³⁰

- Ezt követően kerülhet sor az e-mail fiók használatának magasabb szintű, részletekbe menő ellenőrzésére, azonban itt is ügyelni kell a fokozatosságra, illetve arra, hogy milyen információk állnak a munkáltató rendelkezésére a konkrét jogsértéssel kapcsolatban. Ugyanis ezek az információk befolyásolhatják az ellenőrzés fókuszát, menetét. Így például a munkáltató rendelkezésére állhat az az információ, hogy az e-mailhez csatolt nagy méretű mellékletben továbbítottak egy, az üzleti érdeke szempontjából fontos dokumentumot, és ekkor a forgalmi adatok elemzése útján megállapítható, hogy a levelezőrendszeren keresztül történt-e nagy méretű mellékletet tartalmazó e-mail kiküldése. Ha pedig meghatározott időintervallumban történt jogsértő e-mail kiküldése, akkor nyilvánvalóan elegendő ezen e-mailek áttekintése is. Az e-mailek tartalmának ellenőrzésére is ebben az esetben van lehetősége a munkáltatónak, hiszen ezekkel kapcsolatban már nagy valószínűség szerint kizárható, hogy munkavállaló magánszféráját érintő e-mail tartalmát ismerhetné meg.

Az e-mail fiók használatánál főszabályként biztosítani kell a munkavállaló jelenlétét. A munkáltatói ellenőrzés e formájánál ugyanis a munkavállaló és harmadik személyek különböző személyes adatai lehetnek benne a levelezőrendszerben, amelyek megismerésére a munkáltató nem jogosult. Ha ez ellenőrzésnél a munkavállaló jelen van, és jelezheti valamely email tartalmának megtekintése előtt, hogy azok személyes adatokat tartalmaznak, akkor ezzel biztosítható, hogy a munkáltató ne sértse meg ezt a tilalmat.

Ahhoz, hogy az e-mail fiók ellenőrzése jogszerű legyen, a munkáltatónak előzetesen részletes tájékoztatást kell biztosítania a munkavállalók számára. A tájékoztatóban a munkáltatónak ki kell térnie többek között arra, hogy:

- milyen célból, milyen munkáltatói érdekek miatt kerülhet sor az e-mail fiók ellenőrzésére (illetve természetesen a konkrét ellenőrzés előtt tájékoztatni kell a munkavállalót arról, hogy milyen munkáltatói érdek miatt kerül sor az ellenőrzésre),
- a munkáltató részéről ki végezheti az ellenőrzést,
- milyen szabályok szerint kerülhet sor ellenőrzésre (fokozatosság elvének betartása) és mi az eljárás menete,
- milyen jogai és jogorvoslati lehetőségei vannak a munkavállalóknak az e-mail fiók ellenőrzésével együtt járó adatkezeléssel kapcsolatban.

³⁰ Ezzel kapcsolatban érdemes kiemelni az Mt. 111. § (1) bekezdésben szereplő korlátozó rendelkezést: „a munkavállaló magánélete nem ellenőrizhető.”

A munkahelyi e-mailfiók használatának ellenőrzésével kapcsolatban az Emberi Jogok Európai Bírósága (a továbbiakban: EJEB) a Barbulescu contra Románia-ügyben 2016. január 12. napján hozott ítéletében³¹ megállapította, hogy nem jogsértő, ha a munkáltató megfigyeli egy alkalmazott munkahelyi levelezését. A Hatóság az EJEB döntésének áttekintését³² követően a fent kifejtett álláspontot tartja irányadónak a munkahelyi e-mail fiók használatával kapcsolatban.

4.3. A munkáltató által a munkavállaló rendelkezésére bocsátott laptop ellenőrzése

4.3.1. Előzetes intézkedések

A munkáltató bizonyos munkakörben dolgozó munkavállalók számára „céges laptopot” biztosíthat a munkájuk elvégzéséhez. Ezzel összefüggésben is felmerülhet az a probléma, hogy a laptopot a munkavállalók saját, személyes céljaira is használhatják, amely visszaszerezési helyzetet teremthet abban az esetben, ha a munkáltató a laptop tartalmáról biztonsági mentést kíván készíteni vagy – az Mt. 11. §-ában foglalt jogaival élve – ellenőrizni kívánja a laptopon tárolt adatokat.

A munkáltatónak ezért mindenképp egy belső szabályzatot kell megalkotnia a „céges laptop” használatának, ellenőrzésének szabályairól. Ezzel ugyanis hatékonyan meg lehet előzni azt, hogy a munkavállalók (és adott esetben más érintettek) személyes adatait is kezelje a munkáltató. A belső szabályzatban többek között az alábbiakra szükséges kitérni:

- használható-e magáncélokra a „céges laptop”,
- a laptopról biztonsági mentés készítésének és megőrzésének a szabályozására, illetve arra, hogy mikor kerül sor az e-mailek végleges törlésére,
- a laptopon tárolt adatok ellenőrzésének részletes szabályaira.

Amennyiben a munkáltató engedélyezi a laptop magáncélú használatát, akkor erre vonatkozóan plusz intézkedéseket szükséges meghoznia, így például a laptop merevlemezén több partíciót létrehozni, amellyel biztosítható, hogy a merevlemez egyik részén található a munkavégzéssel összefüggő adatok, míg a másik részén pedig a munkavállaló személyes adatai. Ugyanis mind a laptopról készített biztonsági mentés során, mind a laptop ellenőrzése során a munkáltatónak kiemelt figyelmet kell fordítania arra, hogy a munkavállalók magánélettel kapcsolatos személyes adatait nem kezelheti. Ennek megfelelően úgy kell kialakítani a biztonsági mentés szabályait, hogy az ne terjedjen ki a laptopon tárolt személyes adatokra. Ezen túlmenően a munkáltatói ellenőrzést is úgy kell a munkáltatónak végrehajtania, hogy az ellenőrzés ne érintse a laptopon található személyes adatokat, azokat az ellenőrzéssel összefüggésben nem tárolhatja.³³

³¹ Az EJEB ítélete az alábbi linkről érhető el angol nyelven: <http://hudoc.echr.coe.int/eng?i=001-159906#%7B%22itemid%22:%5B%22001-159906%22%7D>

³² A Hatóság álláspontja szerint a Barbulescu contra Románia-ügyben az EJEB nem az adatvédelem fogalomrendszerében értelmezte a kérdéses problémát, hanem alapjogi kontextusban. Ezzel az EJEB döntése azt megerősítette ugyan, hogy a munkáltatónak jogos érdeke fűződhet az e-mail fiók ellenőrzéséhez, ez azonban az érdekmérlegelési teszt első lépéshez, „az adatkezelői jogos érdek” meghatározásához jelenthet alapot. Adatvédelmi szempontból szükséges a teszt további lépéseinek elvégzése is (munkavállalói érdekek, elvárások meghatározása, súlyozás elvégzése), melyre vonatkozóan az EJEB az ítéletében már nem határozott meg követelményeket.

³³ A laptop munkáltatói ellenőrzésének jogszerűségével szól a Hatóság NAIH/2015/1402/H. számú határozat, amelynek elérhetősége megtalálható jelent tájékoztató IV. pontjában.

4.3.2. Adatvédelmi követelmények

A „céges laptop” tartalmának ellenőrzése esetében a munkáltatói jogos érdek lesz az adatkezelés jogalapja, ezért a munkáltatónak az adatkezelés megkezdése előtt el kell végeznie az érdekmérlegelés tesztjét. Ezen ellenőrzés esetében kiemelt figyelmet kell fordítani az célhoz kötött adatkezelés elvén és a szükségesség-arányosság követelményén túl az érintettek magánszférájára is, hiszen adott esetben különféle, a munkaviszonyhoz nem kapcsolódó személyes adat is a munkáltató tudomására juthat, illetve vele munkaviszonyban nem álló személyek adatait is megismerheti.

Ennek megfelelően a munkáltatónak már előzetesen, a szabályzat megalkotása során meg kell határozni azt, hogy milyen céljai, érdekei miatt kerülhet sor a „céges laptop” tartalmának ellenőrzésére. Ezen érdekeknek ténylegesnek és valósnak, a munkáltató tevékenységéhez, piaci helyzetéhez és a munkavállaló munkaköréhez igazodóknak kell lenniük. Ezen túlmenően a munkáltatónak a laptop tartalmának ellenőrzése előtt közölnie kell a munkavállalóval, hogy pontosan milyen érdeke miatt kerül sor a munkáltatói intézkedésre.

Másrészt a munkáltatónak a fokozatosság elvére figyelemmel lépcsőzetes ellenőrzési rendszert kell kidolgoznia, amelyben megfelelően érvényesülhet a személyes adatok védelme, illetve hogy az ellenőrzés minél kisebb mértékben érintse a munkavállalók magánszféráját. A laptop tartalmának az ellenőrzése során ezért főszabályként biztosítani kell a munkavállalók jelenlétét. A munkáltatói ellenőrzés e formájánál ugyanis a munkavállalók és harmadik személyek különböző személyes adatai lehetnek a laptopon, amelyek megismerésére a munkáltató nem jogosult. Ha az ellenőrzésnél a munkavállaló jelen van, és jelezheti valamely email tartalmának megtekintése előtt, hogy azok személyes adatokat tartalmaznak, akkor ezzel biztosítható, hogy a munkáltató ne sértse meg ezt a tilalmat.

4.3.3. Speciális követelmények, ha a laptop magáncélú használatát nem engedélyezi a munkáltató

Amennyiben a szabályzatban a munkáltató nem engedélyezi a „céges laptop” magáncélú használatát, akkor ebben a munkáltató kifejezetten hívja fel a munkavállalók figyelmét arra, hogy a laptop csak munkavégzéssel összefüggő célokra használható, és a munkáltató valamennyi, a laptopon tárolt adatait ellenőrizheti.

Ebben az esetben a munkavállalók tisztában vannak azzal, hogy személyes adatokat nem tárolhatnak a laptopon, vagy ha ezt mégis megteszik, a munkáltató velük szemben munkajogi jogkövetkezményeket alkalmazhat.

Mint már korábban szó volt róla, a munkáltató ebben az esetben is pusztán azt a tényt rögzítheti, hogy a munkavállalók a laptopon – a belső szabályzat előírásai ellenére – személyes adatokat tároltak, azonban ezen túlmenően a munkáltató nem kezelhet személyes adatokat, tehát azt már nem rögzítheti, hogy a munkavállalók pontosan milyen adatokat is tároltak a gépen (például milyen fényképeket, videókat, dokumentumokat).

4.3.4. Egyéb adatvédelmi követelmények

Ahhoz, hogy a laptop tartalmának az ellenőrzése jogszerű legyen, a munkáltatónak előzetesen részletes tájékoztatást kell biztosítania a munkavállalók számára. A tájékoztatásban a munkáltatónak ki kell térnie többek között arra, hogy:

- hogy milyen célból, milyen munkáltatói érdekek miatt kerülhet sor az laptop ellenőrzésére (illetve természetesen a konkrét ellenőrzés előtt tájékoztatni kell a munkavállalót arról, hogy milyen munkáltatói érdek miatt kerül sor az ellenőrzésre),
- a munkáltató részéről ki végezheti az ellenőrzést,
- milyen szabályok szerint kerülhet sor ellenőrzésre (fokozatosság elvének betartása) és mi az eljárás menete,
- milyen jogai és jogorvoslati lehetőségei vannak a munkavállalóknak a „céges laptop” ellenőrzésével együtt járó adatkezeléssel kapcsolatban.

4.4. Az internethasználat ellenőrizhetősége

Az ellenőrzés e formájával összefüggésben előzetesen érdemes kiemelni, hogy a munkavállaló által meglátogatott weboldal vagy az internethasználatával kapcsolatban a számítógépen rögzített, lementett információk (például az elmentett felhasználónév, jelszó) a munkavállaló személyes adatainak tekinthetők. Ebből fakadóan a munkáltatónak a munkavállalók internethasználatával összefüggésben is tekintettel kell lenniük az adatvédelmi követelményekre.

Az ellenőrzést megelőzően a munkáltatónak célszerű egy belső szabályzatot készítenie, amelyben ki kell térnie többek között:

- arra, hogy mely honlapok megtekintését tiltja (blokkolja) a munkahelyi számítógépeken,
- az ellenőrzés lefolytatására vonatkozó részletes szabályokra.

Amennyiben a munkáltató szabályzata előre meghatározza, hogy mely honlapok megtekintését blokkolja a munkáltató informatikai rendszere, akkor ezzel jelentősen csökkenteni lehet annak esélyét, hogy az internethasználat esetleges ellenőrzésére egyáltalán sor kerüljön.³⁴ Ezzel egyidejűleg ugyanakkor a munkáltatói ellenőrzés lehetőségének is meg kell maradnia, hiszen a munkavállalók adott esetben a tiltást „kijátszhatják” vagy más, a tiltásban nem szereplő, de ahhoz hasonló honlapot tekinthetnek meg a munkahelyükön, amely miatt a munkáltató – az Mt. 11. §-ában foglalt jogával élve – ellenőrizheti, hogy munkavállalók megtartották-e a belső szabályzat előírásait, és adott esetben munkajogi jogkövetkezményt alkalmazhat velük szemben.

Az internethasználat ellenőrzése esetén – mint más munkáltatói ellenőrzéseknél is – szintén a munkáltatói jogos érdek lesz az adatkezelés jogalapja, ennek megfelelően a munkáltatónak el kell végeznie az érdekmérlegelés tesztjét a rendszer bevezetése előtt. Az érdekmérlegelési teszt elvégzése során a munkáltatónak többek között az alábbi követelményeket kell betartania:

- A munkáltatónak előzetesen meg kell határoznia azt, hogy milyen céljai, érdekei miatt kerülhet sor az internethasználat ellenőrzésére. Ezen érdekeknek ténylegesnek és valósnak, a munkáltató tevékenységéhez, piaci helyzetéhez, a munkavállaló munkaköréhez igazodóknak kell lenniük. Ezen túlmenően a munkáltatónak az

³⁴ Az Adatvédelmi Munkacsoport is ezt a megoldást javasolja a munkáltatók számára: 6/2014. számú vélemény 69. oldal.

internethasználat ellenőrzése előtt közölnie kell a munkavállalókkal, hogy pontosan milyen érdekei miatt kerül sor a munkáltatói intézkedésre.

- Az ellenőrzés csak az ahhoz szükséges személyes adatok megismerésére terjedhet ki. Ha például a munkáltató bizonyos honlapok látogatását blokkolja, és az ellenőrzése pusztán arra terjed ki, hogy megállapítsa azt, hogy munkavállaló betartotta-e ezt a munkáltatói rendelkezést, akkor elegendő a honlap címének a megismerése és feljegyzése, és nem szükséges a munkavállaló tevékenységének részletes feltérképezése (mit is csinált a honlapon, milyen felhasználó nevet és jelszavat mentett el, esetleg milyen fájlokat mentett le a honlapról).

Ahhoz, hogy az internethasználat ellenőrzése jogszerű legyen, a munkáltatónak előzetesen részletes tájékoztatást kell biztosítania a munkavállalók számára. A tájékoztatóban a munkáltatónak ki kell térnie többek között arra, hogy:

- hogy milyen célból, milyen munkáltatói érdekek miatt kerülhet sor az internethasználat ellenőrzésére (illetve természetesen a konkrét ellenőrzés előtt tájékoztatni kell a munkavállalót arról, hogy milyen munkáltatói érdekek miatt kerül sor az ellenőrzésre),
- a munkáltató részéről ki végezheti az ellenőrzést,
- milyen szabályok szerint kerülhet sor ellenőrzésre (fokozatosság elvének betartása) és mi az eljárás menete,
- milyen jogai és jogorvoslati lehetőségeik vannak a munkavállalóknak az internet használatának ellenőrzésével együtt járó adatkezeléssel kapcsolatban.

4.5. A „céges mobiltelefon” használatának ellenőrizhetősége

4.5.1. Előzetes intézkedések

Egyre több munkáltatónál elterjedt gyakorlat, hogy „céges mobiltelevont” biztosítanak a munkavállalók számára, amelynek magáncélú használata sok esetben nem tisztázott.

Ezért ebben az esetben szükséges, hogy a munkáltató belső szabályzatban rendelkezzen többek között arról, hogy használható-e magáncélokra a „céges mobiltelefon”, és ha igen, akkor a magáncélú hívások költségeit a munkavállalóknak kell-e viselniük, valamint arra is, hogy milyen esetben kerülhet sor a „céges telefon” használatának ellenőrzésére.

4.5.2. A nem engedélyezett magáncélú telefonhasználat ellenőrzése

Amennyiben a munkáltató nem engedélyezi a „céges mobiltelefon” magáncélú használatát, akkor a munkáltató kifejezetten hívja fel a munkavállalók figyelmét arra, hogy a mobiltelefon csak munkavégzéssel összefüggő célokra használható, és a munkáltató valamennyi kimenő hívás hívószámát és adatait ellenőrizheti.

Ebben az esetben a munkavállalók tisztában vannak azzal, hogy magáncélú hívást nem kezdeményezhetnek, vagy ha ezt mégis megteszik, a munkáltató – élve az Mt. 11. §-ában szereplő ellenőrzési jogával – megismerheti a hívásokat annak érdekében, hogy a magáncélú és a munkavégzési célú telefonhasználatot elkülönítse, illetve a magáncélú hívások tényét deklarálja, bizonyítsa.

Azonban ezen túlmenően a munkáltató nem kezelhet személyes adatokat, tehát azt már nem ismerheti meg, hogy a munkavállalók magáncélból kit és mikor hívtak fel, minthogy ennek megismerése már nem elengedhetetlenül szükséges az ellenőrzés céljához, illetve az Mt. 11. § (1) bekezdése is kimondja azt, hogy a munkavállaló magánélete nem ellenőrizhető.

4.5.3. Az engedélyezett magáncélú telefonhasználat ellenőrzése

Ha a „céges mobiltelefon” magáncélra is használható, akkor a Hatóság jó gyakorlatnak tekinti azt, ha a kimenő hívások két előhívóval vehetőek igénybe: az egyik előhívó a hivatalos, a másik előhívó a magáncélú hívások során használható. A hivatalos hívások adatait a munkáltató megismerheti, a magáncélú hívások adatait nem. A munkáltató ezzel kapcsolatban előírhatja, hogy a magáncélú hívások költségeit a munkavállaló viselje.

A Hatóság emellett a magáncélú telefonhasználat engedélyezése során elfogadhatónak tartja azt is, hogy a munkáltató hívásrészletezőt kér a telefonszolgáltatótól és felhívja a munkavállalót arra, hogy a dokumentumon a magáncélú hívások esetében a hívott számokat tegye felismerhetetlenné. A fennmaradó telefonszámokat a munkáltató megismerheti, hiszen azokat a munkáltató képviselőjében hívta fel a munkavállaló. A munkáltató természetesen ekkor is előírhatja, hogy a magáncélú hívások költségeit a munkavállaló viselje.

A fenti ellenőrzések esetén is érvényes, hogy a munkáltató nem kezelhet személyes adatokat, tehát azt már nem ismerheti meg, hogy a munkavállaló magáncélból kit és mikor hívott fel.

4.5.4. További adatvédelmi követelmények

A „céges mobiltelefon” használatának ellenőrzése esetén ugyancsak a munkáltatói jogos érdek lesz az adatkezelés jogalapja, ennek megfelelően a munkáltatónak el kell végeznie az érdekmérlegelés tesztjét a rendszer bevezetése előtt. Az érdekmérlegelési teszt elvégzése során a munkáltatónak a fent már kifejtett követelményeket kell betartania. Ennek megfelelően a munkáltatónak meg kell határoznia, hogy milyen módon használhatják a munkavállalók a „céges mobiltelefon”, illetve az ellenőrzés is ehhez az előíráshoz kapcsolódhat. Az ellenőrzés nem terjedhet ki arra, hogy a munkavállalók magáncélból kit és mikor hívtak fel.

Mint már korábban, a többi munkáltatói ellenőrzésnél is szó volt róla, az adatkezelés jogszerűségéhez elengedhetetlen, hogy a munkáltató előzetesen részletes tájékoztatást biztosítson a munkavállalók számára. A tájékoztatóban a munkáltatónak ki kell térnie többek között arra, hogy:

- hogy milyen célból, milyen munkáltatói érdekek miatt kerülhet sor a „céges mobiltelefon” használatának ellenőrzésére,
- a munkáltató részéről ki végezheti az ellenőrzést,
- milyen szabályok szerint kerülhet sor ellenőrzésre és mi az eljárás menete,
- milyen jogai és jogorvoslati lehetőségei vannak a munkavállalóknak „céges mobiltelefon” ellenőrzésével együtt járó adatkezeléssel kapcsolatban.

5. GPS navigációs rendszer alkalmazhatósága

A GPS navigációs rendszer által tárolt adat a gépjárművet vezető személyes adatának is minősül, minthogy annak alapján következtetéseket lehet levonni a munkavállalóra (például mikor, milyen útvonalon haladt a munkavállaló, mennyi idő alatt milyen távolságot tett meg).

A GPS alkalmazását a Hatóság logisztikai célból javasolja alkalmazni, a jármű helyzetének a meghatározására kell szolgálnia, nem pedig a munkavállaló követésére. A munkafolyamatok, és ezáltal közvetve a munkavállaló ellenőrzése kizárólag munkával, munkaszervezéssel összefüggő célokat szolgálhat.

A GPS rendszer alkalmazása esetén – mint más munkáltatói ellenőrzéseknél is – szintén a munkáltatói jogos érdek lesz az adatkezelés jogalapja, ennek megfelelően a munkáltatónak el kell végeznie az érdekmérlegelés tesztjét a rendszer bevezetése előtt.

A GPS navigációs rendszer alkalmazása esetében az érdekmérlegelési teszt egyik központi kérdése, hogy milyen cél érdekében kívánja alkalmazni a munkáltató a rendszert, és miért is jelenti e rendszer alkalmazása a munkavállalók személyes adatainak védelméhez fűződő jogának arányos korlátozását. Elfogadható a munkáltató részéről az, ha a rendszer alkalmazásának célja az, hogy a munkáltató egyes munkakörök esetében hatékonyabban szervezze meg a munkafolyamatokat, így például ha a munkáltatónak munkaszervezési szempontból szükséges tudnia azt, hogy egy futár vagy egy fuvarozó az adott időpontban hol jár.

Ezen kívül abban az esetben is jogszerű a GPS alkalmazása, ha a gépjármű szállítmánya, rakománya (így például jelentős összegű készpénz, nagy értékű vagyontárgy, veszélyes áru szállítása), vagy maga a gépjármű, illetve annak értéke ezt kifejezetten indokolja. Jogszerűen alkalmazható GPS továbbá akkor is, ha a munkavállalók életének, testi épségének a megóvása a GPS rendszer alkalmazásának célja (például konfliktus zónán keresztül történő szállítás): amennyiben valamilyen incidens történik, akkor a GPS rendszeren keresztül meg lehet ismerni, hogy merre is járhatott gépjármű a kérdéses időpontban.

Emellett az adatokat az Mt. 11. §-án alapuló munkáltatói ellenőrzés során is fel lehet használni, ha a munkáltató azt tapasztalja, hogy munkavállaló nem teljesítette a munkaviszonyából fakadó kötelezettséget (például a munkavállaló indokolatlanul eltért a munkáltatói utasításba adott útvonaltól).

Ezen túlmenően a GPS navigációs rendszer jogszerű alkalmazásához is szükséges, hogy a munkáltató megfelelő tájékoztatást biztosítson a munkavállalók részére, így a tájékoztatónak többek között ki kell térnie arra, hogy

- hogy milyen célból, milyen munkáltatói érdekek miatt kerülhet sor az GPS navigációs rendszer adatainak felhasználására,
- a munkáltató részéről ki férhet hozzá ezen adatokhoz,
- milyen szabályok szerint kerülhet sor az adatok megismerésére, és mi az eljárás menete
- amennyiben a munkáltató az Mt. 11. §-ával összhangban végez ellenőrzést, akkor szabályaira (a fokozatosság elvének betartása) és mi az eljárás menete, ki végezheti az ellenőrzést a munkáltató részéről,
- milyen jogai és jogorvoslati lehetőségei vannak a munkavállalónak a GPS rendszer alkalmazásával együtt járó adatkezeléssel kapcsolatban.

Az ellenőrzés csak munkaidőben történhet és nem ellenőrizhető a munkavállalók földrajzi helyzete munkaidőn kívül. Egy olyan gépjármű esetében, amellyel jelentős értékű anyagot nem szállítanak, vagy az adott munkavállaló a munkáját otthonában, „home office”-ban látja el, a GPS alkalmazása nem indokolt. Ez azt jelenti, hogy a munkavállalónak lehetőséget kell adni arra, hogy a GPS-t kikapcsolja akkor is, ha az nála marad (például ha a járművet munkaidőn kívül is magánál tarthatja).

6. Biometrikus rendszerek alkalmazhatósága

6.1. A biometrikus rendszer

Az Adatvédelmi Munkacsoport a 3/2012. számú véleményében³⁵ meghatározta a biometrikus adatok két fő kategóriáját:

- Egyrészt vannak fizikai és fiziológiai alapú technikák, amelyek a személyek fizikai és fiziológiai jellemzőit vizsgálják (például az ujjlenyomat-ellenőrzés).
- Másrészt vannak a viselkedésen alapuló technikák, amelyek a személyek viselkedését mérik, ide tartozik például a gépírás elemzése, a valamilyen tudatalatti gondolatra, például hazugságra utaló mintázatok.

A biometrikus rendszerek olyan biometrikus adatokat használó alkalmazások, amelyek lehetővé teszik a személyek automatikus azonosítását, illetve hitelesítését, ellenőrzését. A biometrikus rendszereken keresztül végzett adatkezelés különböző folyamatokat foglal magában, így a felvételt, a tárolást és a megfeleltetést.

- Biometrikus felvétel: a biometrikus adatok valamely biometrikus forrásból való kinyerése és azoknak egy egyénhez való kapcsolása. A felvételi szakasz tipikusan az első alkalom, amikor egy egyén kapcsolatba kerül egy adott biometrikus rendszerrel. A felvételhez a legtöbb esetben az egyén személyes közreműködése szükséges (például ujjlenyomatvétele esetén), ami megfelelő alkalmat adhat a tájékoztatásra és a tisztességes adatfeldolgozásról szóló tájékoztatásra.
- Biometrikus tárolás: a felvétel során megszerzett adatok későbbi felhasználás céljából tárolhatók helyben, abban a műveleti központban, ahol a felvételre sor került (például egy olvasóban), vagy az egyén által hordozott valamely eszközön (például egy intelligens kártyán), illetve elküldhető tárolásra egy központosított adatbázisba, amely hozzáférhető egy vagy több biometrikus rendszer számára.

³⁵ Az Adatvédelmi Munkacsoport több dokumentumában is foglalkozott a biometrikus adatok elektronikus olvasására és feldolgozására képes jövőbeli technológiák használatához kapcsolódó adatvédelmi kérdésekkel, így például a biometrikus technológiák terén történt fejleményekről szóló 3/2012. számú vélemény (a továbbiakban: 3/2012. számú vélemény). Ebben a véleményben a Munkacsoport tisztáz néhány alapfogalmat a biometrikus adatkezeléssel összefüggésben, példák segítségével részletes jogi elemzést nyújt arról, milyen adatvédelmi követelmények megtartása mellett lehet biometrikus adatkezelést végezni, illetve a Munkacsoport kitér arra is, hogy milyen új területei vannak és lesznek a biometrikus adatkezelésnek.

- Biometrikus megfeleltetés: ez az a folyamat, amelynek során a (felvételnél rögzített) biometrikus adatokat (sablon) összevetik egy új mintából gyűjtött biometrikus adatokkal (sablonnal) azonosítás, ellenőrzés (hitelesítés) vagy kategorizálás céljából.

6.2. Előzetes adatvédelmi követelmények

Az Adatvédelmi Munkacsoport a 3/2012. számú véleményében számos adatvédelmi követelményt támaszt a biometrikus rendszerek alkalmazásával kapcsolatban. A munkáltatónak a 3/2012. számú véleményben kifejtett valamennyi követelménynek meg kell felelnie ahhoz, hogy a biometrikus rendszer alkalmazása jogszerű legyen.

Ezen követelmények közül jelen tájékoztatóban az arányosság szerepel kiemelten mint amely az egyik legfontosabb kérdése az ilyen rendszerekkel együtt járó adatkezeléseknek. Egy biometrikus rendszer megfelelőségének értékelése és az arányosság elemzése során előzetesen az alábbiakat kell mérlegelni:

- A rendszer szükséges-e a meghatározott igény kielégítéséhez, azaz használata elengedhetetlen-e ehhez, vagy inkább annak legkényelmesebb vagy legköltséghatékonyabb módja.
- A rendszer valószínűleg elég hatékony lesz-e az adott igény kielégítésében, tekintettel a használni tervezett biometrikus technológia sajátos jellemzőire.
- Arányos-e az elvárt előnyökkel, ha a rendszer miatt sérül a magánélet védelme. Ha az előnyök viszonylag kisebbek, például kényelmesebb az eljárás vagy kismértékű költségmegtakarítás érhető el, akkor nem helyénvaló, ha sérül a magánélet védelme.
- Annak megfontolása, hogy a magánéletbe kisebb mértékben beavatkozó módszerek elérhetnék-e a kívánt célt.

Az arányosság elvének egyik központi kérdése, hogy van-e alternatívája a biometrikus rendszer alkalmazásának. Az adatkezelő minden esetben köteles ellenőrizni, hogy egyes alternatív intézkedések lehetnének-e a kitűzött célra tekintettel ugyanolyan hatékonyak, de kisebb beavatkozással járók, és köteles ezeket az alternatívákat választani.

Természetesen vannak esetek, amikor a biometrikus rendszerek használata az adatkezelő jogszerű érdekét szolgálja. Az ilyen érdek azonban csak akkor jogszerű, ha az adatkezelő bizonyítani tudja, hogy az érdeke objektív módon magasabb rendű az érintett azon jogánál, hogy ne vegyék fel egy biometrikus rendszerbe. A Munkacsoport a 6/2014. számú véleményében hoz erre olyan példát, amelyik illeszkedik a munkahelyi adatkezelés világába: egy tudományos kutatólaboratórium, amely halálos vírusokkal dolgozik, biometrikus beléptetési rendszert használ, mivel ha ezek a vírusok kiszabadulnak a laboratóriumból, igen nagy kockázatot jelentenének a közegészségügyre. Megfelelő biztosítékokat alkalmaznak, ideértve azt, hogy a biometrikus adatokat nem egy központi rendszerben, hanem a munkavállalók személyes belépőkártyáin tárolják. Még ha az adatok tágabb értelemben érzékenyek bizonyulnak is, az adatkezelés közérdeket szolgál. A fent említett indok és azon tény alapján, hogy a biztosítékok megfelelő használata csökkenti a visszaélések kockázatát, az Adatvédelmi Irányelv 7. cikk f) pontja megfelelő jogalapot nyújt az adatkezeléshez.

A fentiek alapján megállapítható, hogy általánosságban a biometrikus rendszerek alkalmazása nem elengedhetetlen és nem a legkíméletesebb eszköz a munkavállalók ellenőrzésénél. Így például az ujjlenyomatos munkaidő-nyilvántartással kapcsolatban megállapítható, hogy a munkavállalók ellenőrzését mint célt más, a magánszférát kímélőbb módszerekkel is el lehet érni, ezért ebből a célból nem lehet biometrikus rendszert bevezetni.

7. A belső visszaélés-bejelentési rendszer (whistleblowing) adatvédelmi követelményei

7.1. A visszaélés-bejelentési rendszer

Ez egy olyan belső jelentéstételi rendszer, amelyen keresztül jelezni lehet a jogszabálysértő vagy a munkáltató magatartási szabályait sértő cselekményeket, és ezen bejelentéseket aztán vagy a munkáltató vagy egy külső szervezet vizsgálja.

Bejelentést bárki tehet, akinek a bejelentés megtételéhez vagy a bejelentés tárgyát képező magatartás orvoslásához méltányolható jogos érdeke fűződik (így például a munkavállalók, a munkáltatóval szerződéses viszonyban álló személyek).

7.2. Követelmények

- A munkáltatónak a visszaélés-bejelentési rendszer működésére, valamint a bejelentéssel kapcsolatos eljárásra vonatkozóan részletes, magyar nyelvű tájékoztatót kell készítenie, illetve azt a honlapján közzé kell tennie. Emellett, ha a munkáltató rendelkezik magatartási szabályokkal, akkor ezt is nyilvánosságra kell hoznia a honlapon (a Pktv. nem kötelezi a munkáltatókat arra, hogy a belső visszaélés-bejelentési rendszer létrehozása érdekében magatartási szabályokat alkossanak meg).
- A Hatóság álláspontja szerint az a tájékoztatás elfogadható, amely megfelelő részletességgel és pontossággal összefoglalja az eljárási szabályokat és a bejelentési rendszer működését, fenntartva a munkáltató számára annak lehetőségét, hogy a számára lényeges – akár az üzleti titok fogalmába tartozó – információkat ne hozza nyilvánosságra, feltéve, hogy az információk elhagyása nem lehetetleníti el a visszaélés-bejelentési rendszer lényeges körülményeiről való tájékozódást.
- Nem megfelelő, ha a tájékoztatást csupán a cég belső-intranetén teszik elérhetővé. Ez következik a Pktv. rendelkezéseiből is, melyek azt a kötelezettséget róják a munkáltatóra, hogy a visszaélés-bejelentési rendszerrel összefüggő tájékoztatókat (magatartási szabályokat, eljárásra vonatkozó szabályokat) a munkáltató a saját, nyilvános, bárki számára elérhető honlapján hozza nyilvánosságra. Ennek az is az indoka, hogy a Pktv. szabályozása alapján a bejelentési rendszerbe nem csak a munkavállalók, hanem a munkáltatóval munkaviszonyon kívüli más, szerződéses viszonyban álló, vagy olyan személyek is tehetnek bejelentést, akiknek a bejelentés megtételéhez vagy a bejelentés tárgyát képező magatartás orvoslásához méltányolható jogos érdekük fűződik. Ennek megfelelően tehát a foglalkoztatói szervezeteknek sokkal szélesebb személyi kör számára kell tájékoztatást nyújtaniuk, hiszen olyan személyek is tehetnek bejelentést (például beszállítók, alvállalkozók), akik a belső hálózathoz (intranethez) adott esetben nem férhetnek hozzá. A Pktv. rendelkezéseinek sérelmét jelentené az a gyakorlat, ha ezen tájékoztatókat a munkáltató kizárólag az intraneten keresztül tenné közzé.

- A munkáltatónak a bejelentési rendszerhez kapcsolódó adatkezelést be kell jelentenie a Hatóság által vezetett adatvédelmi nyilvántartásba. Ennek során az Infotv. 65. § (3) bekezdés a) pontjában megfogalmazott kivételszabályt nem lehet alkalmazni.

7.3. A kezelhető személyes adatok köre és ideje

- A bejelentés megtételekor a bejelentő a nevét és lakcímét, jogi személy bejelentő esetén annak székhelyét és a bejelentést benyújtó törvényes képviselőjének nevét köteles megadni. Emellett a bejelentőnek nyilatkoznia kell arról, hogy a bejelentést jóhiszeműen teszi olyan körülményekről, amelyekről tudomása van, vagy kellő alappal feltételezi, hogy azok valósak. A Pktv. egyébként felhatalmazást biztosít a bejelentőnek, valamint a bejelentésben érintett személynek a bejelentésben megadott személyes adatainak a bejelentés kivizsgálása céljából történő kezelésére.
- A Pktv. rendelkezései szerint a bejelentési rendszerben különleges adatok kezelése tilos. A Pktv. 14. § (3) bekezdése egyértelmű jogalkotói rendelkezés, amely felülírja az Infotv. rendelkezéseinek alkalmazását, mind a kezelhető adatok, mind pedig az alkalmazható jogalapok tekintetében. Ennek megfelelően, mivel a jogalkotó kategorikusan kizárta annak lehetőségét, hogy a visszaélés-bejelentési rendszeren keresztül különleges adatokat kezeljenek, ezért a visszaélés-bejelentési rendszert úgy kell kialakítani, hogy annak keretében a munkáltató különleges adatokat ne kezelhessen.
- A bejelentési rendszerből haladéktalanul törölni kell a bejelentésben nem érintett harmadik személyre vonatkozó, a bejelentés kivizsgálásához nem szükséges, valamint a Pktv. szerint nem kezelhető adatokat.
- A Pktv. meghatározza a személyes adatok kezelésének lehetséges időtartamát. Eszerint a bejelentés kivizsgálására alapvetően 30 nap áll rendelkezésre, de a vizsgálat legfeljebb 3 hónapig tarthat. Ezt követően dönteni kell, hogy a munkáltató alkalmaz-e intézkedést a bejelentés alapján. Amennyiben igen, akkor a vizsgálat alapján megismert személyes adatokat a bejelentés alapján indított eljárások jogerős lezárásáig lehet kezelni. Azonban ha a vizsgálat alapján a bejelentés nem megalapozott vagy további intézkedés megtétele nem szükséges, akkor a személyes adatokat 60 napon belül törölni kell.

7.4. Adatvédelmi követelmények

- A visszaélés-bejelentési rendszer esetében nem csak a bejelentő számára kell tájékoztatást nyújtani az adatkezelésről, hanem a Pktv. kifejezett tájékoztatási kötelezettséget ír elő a bejelentésben érintett személy esetében is, akit a vizsgálat megkezdésekor részletesen tájékoztatni kell a rá vonatkozó bejelentésről, az Infotv. alapján megillető jogairól, valamint az adatai kezelésére vonatkozó szabályokról.
- A bejelentési rendszert úgy kell kialakítani, hogy a nem névtelen bejelentő személyét a bejelentést vizsgálókon kívül más ne ismerhesse meg. A bejelentést vizsgálók a vizsgálat lezárásáig vagy a kivizsgálás eredményeképpen történő formális felelősségre vonás kezdeményezéséig a bejelentés tartalmára és a bejelentésben érintett személyekre vonatkozó információkat kötelesek titokban tartani, és azokat – a bejelentésben érintett

személy tájékoztatása kivételével – nem oszthatják meg a foglalkoztatói szervezet egyetlen más szervezeti egységével vagy munkatársával sem

- Amennyiben a visszaélés-bejelentési rendszerrel összefüggésben személyes adatok külföldi továbbítására is sor kerül, akkor alkalmazni kell az Infotv. 8. § (2) bekezdését.

Budapest, 2016. október 28.

Dr. Péterfalvi Attila
elnök
c. egyetemi tanár

III. Jogszabályjegyzék

A tájékoztatóban hivatkozott uniós jogszabályok:

- Az Európai Parlament és a Tanács 95/46/EK számú, a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló irányelv (**Adatvédelmi Irányelv**)
- A Bizottság 2016/1250 végrehajtási határozata a 95/46/EK európai parlamenti és tanácsi irányelv alapján az EU–USA adatvédelmi pajzs által biztosított védelem megfelelőségéről (**Privacy Shield határozat**)

A tájékoztatóban hivatkozott magyar jogszabályok:

- Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (**Infotv.**)
- A Munka Törvénykönyvéről szóló 2012. I. számú törvény (**Mt.**)
- A személy-és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól szóló 2005. évi CXXXIII. törvény rendelkezései (**Szvtv.**)
- A bűnügyi nyilvántartási rendszerről, az Európai Unió tagállamainak bíróságai által magyar állampolgárokkal szemben hozott ítéletek nyilvántartásáról, valamint a bűnügyi és rendészeti biometrikus adatok nyilvántartásáról szóló 2009. évi XLVII. törvény (**Bnyt.**)
- A közalkalmazottak jogállásáról szóló 1992. évi XXXIII. törvény (**Kjt.**)
- A panaszokról és a közérdekű bejelentésekről szóló 2013. évi CLXV. törvény (**Pktv.**)
- A munkaerő-kölcsönzési és a magán-munkaközvetítói tevékenység nyilvántartásba vételéről és folytatásának feltételeiről szóló 118/2001. (VI. 30.) Korm. rendelet [**118/2001. (VI. 30.) Korm. rendelet Korm. rendelet**]

IV. Egyéb joganyagok

A Hatóságnak a tájékoztatóban hivatkozott ajánlásai, határozatai, állásfoglalásai:

- A munkahelyen alkalmazott elektronikus megfigyelőrendszer alapvető követelményeiről szóló ajánlás: <http://naih.hu/files/Ajanlas-a-munkahelyi-kameras-megfigyelesr-l.pdf>
- Az előzetes tájékoztatás adatvédelmi követelményeiről szóló ajánlás: <http://naih.hu/files/tajekoztato-ajanlas-v-2015-10-09.pdf>
- Az anonim álláshirdetések jogszerűségéről szóló NAIH-1159-15/2015/H. számú határozat: http://naih.hu/files/NAIH-2015-1159-H_hatarozat_anonim.pdf
- A munkáltató által a munkavállaló rendelkezésére bocsátott laptop ellenőrzéséről szóló NAIH/2015/1402/H. számú határozat: http://naih.hu/files/2355_2014_H_hat_anonim.pdf
- Állásfoglalás a külföldi adattovábbítás alapvető követelményeiről: <http://naih.hu/files/2223-2-2013-v.pdf>

Az Adatvédelmi Munkacsoportnak a tájékoztatóban hivatkozott joganyagai:

- 8/2010. számú vélemény az alkalmazandó jogról (**8/2010. számú vélemény**): http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp179_hu.pdf
- 15/2011. számú vélemény a hozzájárulás fogalom-meghatározásáról (**15/2011. számú vélemény**): http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_hu.pdf
- 3/2012. számú vélemény a biometrikus technológiák terén történt fejleményekről (**3/2012. számú vélemény**): http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_hu.pdf
- 6/2014. számú vélemény az adatkezelő 95/46/EK irányelv 7. cikke szerinti jogszerű érdekeinek fogalmáról (**6/2014. számú vélemény**): http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_hu.pdf

Az Európai Unió Bíróságának a tájékoztatóban hivatkozott döntései:

- C-468/10. és C-469/10. sz. ügy: Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) és Federación de Comercio Electrónico y Marketing Directo (FECEDM) (C-469/10) kontra Administración del Estado egyesített ügyekben hozott ítélet: <http://curia.europa.eu/juris/document/document.jsf?jsessionid=9ea7d2dc30d5cd3639833c864d7aa216963d279ce13b.e34KaxiLc3qMb40Rch0SaxyKaNb0?text=&docid=115205&pageIndex=0&doclang=HU&mode=lst&dir=&occ=first&part=1&cid=252119>

- C-131/12. sz. ügy: Google Spain SL és Google Inc. kontra Agencia Española de Protección de Datos (AEPD) és Mario Costeja González ügyben hozott ítélet:
<http://curia.europa.eu/juris/document/document.jsf?jsessionid=9ea7d2dc30d5997afa8511b4499ab49ea6a6560b9b10.e34KaxiLc3qMb40Rch0SaxyKaN10?text=&docid=152065&pageIndex=0&doclang=HU&mode=lst&dir=&occ=first&part=1&cid=694361>