A 29. CIKK SZERINTI ADATVÉDELMI MUNKACSOPORT

17/HU

WP 249

2/2017. számú vélemény a munkahelyi adatkezelésről

Elfogadás időpontja: 2017. június 8.

Tartalom

1. Vezetői összefoglaló

Ez a vélemény kiegészíti a 29. cikk szerinti adatvédelmi munkacsoport (a továbbiakban: munkacsoport) korábbi kiadványait: *a személyes adatok munkaviszonnyal összefüggő kezeléséről szóló 8/2001. sz. véleményt* (WP48)[1], és *az elektronikus kommunikáció munkahelyi megfigyeléséről szóló 2002. évi munkadokumentumot* (WP55)[2]. E dokumentumok közzététele óta olyan technológiák terjedtek el, amelyek lehetővé teszik a munkavállalók személyes adatainak korábbinál szisztematikusabb kezelését a munkahelyen, jelentős kihívásokat teremtve a magánélet védelme és az adatvédelem szempontjából.

Ebben a véleményben újra felmérjük a munkáltatók jogos érdekei és a munkavállalók magánélet védelmére vonatkozó ésszerű elvárásai közötti egyensúlyt, azzal, hogy felvázoljuk az új technológiák jelentette kockázatokat, és az arányosság szempontjából értékeljük e technológiák alkalmazásának egyes eseteit.

Bár a vélemény elsősorban az adatvédelmi irányelvet veszi figyelembe, az általános adatvédelmi rendelet által a munkáltatókra rótt pluszkövetelményeket is vizsgálja. Emellett megismétli a 8/2001 sz. vélemény és a WP55 munkadokumentum állásfoglalásait és következtetéseit, azaz azt, hogy a munkavállalók személyes adatainak kezelése során:

- a munkáltatónak mindig figyelemmel kell lennie az adatvédelem alapvető elveire, függetlenül az alkalmazott technológiától;
- a vállalati létesítményekből indított elektronikus közlések tartalmára ugyanúgy vonatkozik az alapvető jogok védelme, mint az analóg közlésekre;
- rendkívül valószínűtlen, hogy a jóváhagyás alkalmas jogalap a munkahelyi adatkezeléshez, kivéve, ha a munkavállalók hátrányos következmények nélkül visszautasíthatják;
- esetenként hivatkozni lehet a szerződés teljesítésére vagy a jogos érdekekre, feltéve, hogy az adatkezelés a törvényes cél érdekében feltétlenül szükséges, és megfelel az arányosság és a szubszidiaritás elvének;
- a munkavállalóknak érdemi tájékoztatást kell nyújtani az alkalmazott megfigyelésről; továbbá
- a munkavállalók adatainak nemzetközi továbbítása csak megfelelő szintű védelem biztosítása mellett végezhető.

2. Bevezetés

Az új információs technológiák gyors terjedése a munkahelyeken, legyen szó az infrastruktúráról, alkalmazásokról vagy okoseszközökről, a szisztematikus, potenciálisan zavaró munkahelyi adatkezelés új módozatait teszi lehetővé. Például:

---

[1] *A 29. cikk szerinti munkacsoport 08/2001. sz. véleménye a személyes adatok munkaviszonnyal összefüggő kezeléséről* (WP48), 2001. szeptember 13.; url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2001/wp48_en.pdf

[2] *A 29. cikk szerinti munkacsoport munkadokumentuma az elektronikus kommunikáció munkahelyi megfigyeléséről* (WP55), 2002. május 29.; url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2002/wp55_en.pdf

- a munkahelyi adatkezelést lehetővé tévő technológiák bevezetése ma már a néhány évvel ezelőtti költségek töredékéért megoldható, a technológiák személyesadat-feldolgozási kapacitása pedig exponenciálisan megnőtt;
- az adatkezelés új formái, például az online szolgáltatások igénybe vételével kapcsolatos személyes adatok és/vagy az okoseszközökről származó, tartózkodási helyre vonatkozó adatok kezelése sokkal kevésbé látható a munkavállalók számára, mint más, hagyományosabb módszerek, például a jól láthatóan elhelyezett biztonsági kamerák. Ez felveti azt a kérdést, hogy a munkavállalók mennyire vannak tudatában az ilyen technológiák alkalmazásának, hiszen a munkáltatók az ilyen adatkezelést jogszerűtlenül, a munkavállalók előzetes értesítése nélkül is alkalmazhatják; továbbá
- egyre inkább elmosódik az otthon és a munkahely közötti határ. Amikor például a munkavállalók távolról (például otthonról) dolgoznak, vagy munkaügyben utaznak, a fizikai munkakörnyezeten kívül végzett tevékenységüket is megfigyelhetik, ami akár az adott személy magánjellegű tevékenységének megfigyelését is magában foglalhatja.

Ezért, bár az ilyen technológiák használata segíthet felismerni és megakadályozni a vállalat szellemi és fizikai tulajdonát érintő veszteségeket, valamint fokozni a munkavégzés hatékonyságát és azoknak a személyes adatoknak a védelmét, amelyekért az adatkezelő felelősséggel tartozik, egyben jelentős kihívásokat is eredményez a magánélet védelme és az adatvédelem terén. Ennek következtében újra kell értékelni a munkáltatónak a vállalat védelméhez fűződő jogos érdekei és az érintettek, azaz a munkavállalók magánélet védelmére vonatkozó ésszerű elvárásai közötti egyensúlyt.

A vélemény az új információs technológiákra összpontosít azzal, hogy kilenc különböző helyzetet értékel, amelyben ilyeneket alkalmaznak, de emellett röviden a munkahelyi adatkezelés olyan hagyományosabb módszereire is kitér, ahol a kockázat a technológiai változások következtében megemelkedett.

A munkacsoport a véleményben használt „munkavállaló” szó értelmét nem kívánja leszűkíteni azokra, akik munkaszerződéssel rendelkeznek, és akik a hatályos munkaügyi jogszabályok értelmében munkavállalónak minősülnek. Az elmúlt évtizedek során elterjedtté váltak a munkavégzés különböző formáira épülő üzleti modellek, így különösen az önálló vállalkozók igénybe vétele. Ez a vélemény le kíván fedni minden olyan helyzetet, ahol munkaviszony áll fenn, függetlenül attól, hogy ez a viszony munkaszerződésen alapul-e.

Fontos kimondani, hogy a munkavállalók a munkáltató és a munkavállalók közötti függőségi viszonyból eredően ritkán vannak abban a helyzetben, hogy szabadon megadják, megtagadják vagy visszavonják a hozzájárulásukat. Kivételes helyzetektől eltekintve a munkáltatóknak más, a hozzájárulástól eltérő jogalapra kell támaszkodniuk, mint például az adatok munkáltató jogos érdekei céljából történő kezelése. A jogos érdek megléte azonban önmagában nem elégséges ahhoz, hogy az elsőbbséget élvezzen a munkavállalók jogaival és szabadságaival szemben.

Függetlenül az adatkezelés jogalapjától, az adatkezelés megkezdése előtt meg kell vizsgálni az arányossági feltétel teljesülését, azaz meg kell állapítani, hogy az adatkezelés szükséges-e valamely törvényes cél eléréséhez, és meg kell határozni azokat az intézkedéseket, amelyeket meg kell tenni annak biztosításához, hogy a magánélet tiszteletben tartásához és a közlés titkosságához való jog megsértése a minimális mértékre korlátozódjon. Ez az adatvédelmi hatásvizsgálat részét képezheti.

3. Jogszabályi keretek

Bár az alábbi elemzés elsősorban a 95/46/EK irányelv[3] (a továbbiakban: adatvédelmi irányelv) által meghatározott jelenlegi jogszabályi keretrendszeren alapul, a vélemény figyelembe veszi a már hatályba lépett, 2018. május 25-étől alkalmazandó 2016/679 rendelet[4] (a továbbiakban: általános adatvédelmi rendelet) által előírt kötelezettségeket is.

A javasolt elektronikus hírközlési adatvédelmi rendelet[5] kapcsán a munkacsoport felkéri az európai jogalkotókat, hogy határozzanak meg specifikus kivételt a munkavállalóknak kiadott eszközöket érintő beavatkozások tekintetében[6]. A javasolt rendelet nem tartalmaz megfelelő kivételt a beavatkozás általános tilalma alól, a munkáltatók pedig rendszerint nem tudnak érvényes hozzájárulást adni a munkavállalóik személyes adatainak kezeléséhez.

3.1 A 95/46/EK irányelv (adatvédelmi irányelv)

A munkacsoport a 08/2001. sz. véleményében már megfogalmazta, hogy a személyes adatok munkaviszonnyal összefüggő kezelése esetén a munkáltatónak figyelembe kell vennie az adatvédelmi irányelv alapvető adatvédelmi elveit. Az új technológiák létrejötte és az ilyen adatkezelésre szolgáló új módszerek kifejlesztése ezen nem változtatott — sőt, elmondható, hogy ezek a változások *még* fontosabbá teszik, hogy a munkáltatók ennek megfelelően járjanak el. A munkáltatóknak ezzel összefüggésben:

- biztosítaniuk kell, hogy az adatok kezelése meghatározott, törvényes, arányos és szükséges célból történjen;
- figyelembe kell venniük a célhoz kötöttség elvét, és gondoskodniuk kell arról, hogy az adatok a törvényes cél szempontjából megfelelőek, relevánsak és nem túlzott mértékűek legyenek;
- a jogalaptól függetlenül alkalmazniuk kell az arányosság és a szubszidiaritás elvét;
- biztosítaniuk kell az átláthatóságot a munkavállalók felé a megfigyelési technológiák alkalmazása és célja tekintetében;
- lehetővé kell tenniük az érintettek számára, hogy gyakorolhassák a jogaikat, beleértve a személyes adatokhoz való hozzáféréshez, illetve azok helyesbítéséhez, törléséhez és zárolásához való jogot;
- fenn kell tartaniuk az adatok pontosságát, és nem őrizhetik meg az adatokat a szükségesnél tovább; továbbá
- meg kell tenniük minden szükséges intézkedést az adatok jogosulatlan hozzáférés elleni védelme érdekében, és biztosítaniuk kell, hogy a munkatársaik kellően tisztában legyenek az adatvédelmi kötelezettségekkel.

---

[3] Az Európai Parlament és a Tanács 95/46/EK irányelve (1995. október 24.) a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról, *HL L 281., 1995.11.23., 31-50. o.*, url: http://eur-lex.europa.eu/legal-content/HU/TXT/?qid=1510829604244&uri=CELEX:31995L0046.

[4] Az Európai Parlament és a Tanács 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet) *HL L 119., 2016.5.4., 1-88. o.*, url: http://eur-lex.europa.eu/legal-content/HU/TXT/?qid=1510829556181&uri=CELEX:32016R0679.

[5] Javaslat az Európai Parlament és a Tanács rendeletére az elektronikus hírközlési ágazatban a magánélet tiszteletben tartásáról és a személyes adatok védelméről, valamint a 2002/58/EK irányelv hatályon kívül helyezéséről, 2017/0003 (COD), url: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=41241.

[6] Lásd a 29. cikk szerinti munkacsoport *01/2017. sz. véleményét az elektronikus hírközlési adatvédelmi rendeletre vonatkozó javaslatról*, WP 247, 2017. április 4., 29. o.; url: http://ec.europa.eu/newsroom/document.cfm?doc_id=44103

Anélkül, hogy megismételné a korábban adott tanácsot, a munkacsoport ki szeretne emelni három elvet: a jogalapot, az átláthatóságot és az automatizált döntéseket.

3.1.1 *JOGALAP (7. CIKK)*

A személyes adatok munkaviszonnyal összefüggő kezelése esetén a 7. cikkben felsorolt kritériumok legalább egyikének teljesülnie kell. A (8. cikkben részletezett) különleges személyes adatok kezelése tilos, kivéve, ha valamely kivétel fennáll[7,8]. Az adatkezelés azonban abban az esetben is csak a 7. cikk szerinti jogalapok valamelyikének megléte esetén jogszerű, ha a munkáltató valamely kivételre támaszkodhat.

Összefoglalva, a munkáltatóknak az alábbiakkal kell tisztában lenniük:

- a munkahelyi adatkezelés legtöbb esetében a munkáltató és a munkavállaló közötti viszony jellegéből adódóan a **jogalap nem lehet és nem is lehetne a munkavállaló jóváhagyása** (7. cikk a) pontja);
- az adatkezelés szükséges lehet **szerződés teljesítéséhez** (7. cikk b) pontja), amennyiben ilyen kötelezettség teljesítéséhez a munkáltatónak a munkavállaló személyes adatait kell kezelnie;
- meglehetősen gyakori, hogy a **foglalkoztatási jogszabályok olyan jogi kötelezettségeket** (7. cikk c) pontja) **írnak elő, amelyek személyes adatok kezelését teszik szükségessé;** ebben az esetben a munkavállalót egyértelműen és teljes körűen tájékoztatni kell az adatfeldolgozásról (kivéve, ha erre vonatkozó kivétel áll fenn);
- amennyiben a munkáltató **jogos érdekre** (7. cikk f) pontja) kíván hivatkozni, az adatkezelés céljának jogszerűnek kell lennie; a választott módszernek/technológiának szükségesnek és arányosnak kell lennie, és azt úgy kell alkalmazni, hogy a lehető legkisebb mértékben hatoljon be a magánszférába; továbbá a munkáltatónak képesnek kell lennie igazolni azt, hogy **megfelelő intézkedéseket tett** az egyensúly biztosítására a munkavállalók alapvető jogai és szabadságai tekintetében[9];
- az adatkezelési műveleteknek meg kell felelniük továbbá az **átláthatóság követelményeinek** (10. és 11. cikk), és a munkavállalókat egyértelműen és teljes körűen tájékoztatni kell a személyes adataik kezeléséről[10], beleértve az esetleges megfigyelés alkalmazását; továbbá
- **megfelelő műszaki és szervezeti intézkedéseket** kell alkalmazni az adatkezelés biztonságának biztosítására (17. cikk).

A 7. cikk leglényegesebb kritériumait az alábbiakban részletezzük.

- **Jóváhagyás (7. cikk a) pont)**

[7] Amint azt a 08/2001 sz. vélemény 8. része rögzíti; a 8. cikk (2) bekezdésének b) pontja például kivételt fogalmaz meg arra az esetre, amikor az adatfeldolgozás az adatkezelő kötelezettségei és meghatározott jogai gyakorlása érdekében szükséges a foglalkoztatási jogszabályok területén, amennyiben a megfelelő biztosítékokról rendelkező nemzeti jogszabályok ezt lehetővé teszik.

[8] Megjegyzendő továbbá, hogy egyes országokban különleges intézkedések vannak érvényben, amelyeket a munkáltatóknak a munkavállalók magánélete védelmében be kell tartaniuk. Ilyen különleges intézkedések vannak életben például Portugáliában, és más tagállamok is rendelkezhetnek hasonlókkal. Emiatt a vélemény 5.6 pontjában foglalt következtetések és az 5.1 és 5.7.1 pontjában foglalt példák Portugáliára nem érvényesek.

[9] A 29. cikk szerinti munkacsoport *06/2014. sz. véleménye az adatkezelő jogos érdekének 95/46/EK irányelv 7. cikke szerinti fogalmáról*, WP 217, elfogadás időpontja: 2014. április 9., url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf.

[10] Az adatvédelmi irányelv 11. cikk (2) bekezdése értelmében az adatkezelő mentesül az érintettek tájékoztatásának kötelezettsége alól, ha az adatok rögzítését vagy gyűjtését jogszabály kifejezetten előírja.

Az adatvédelmi irányelv meghatározása szerint a jóváhagyás az érintett kívánságának önkéntes, kifejezett és tájékozott kinyilvánítása, amellyel beleegyezését adja az őt érintő személyes adatok feldolgozásához. A beleegyezés csak akkor érvényes, ha az vissza is vonható.

A munkacsoport a 8/2001. sz. véleményében már rögzítette, hogy azon esetekben, amikor a munkáltatónak kezelnie kell a munkavállalói személyes adatait, félrevezető abból kiindulni, hogy az adatkezelés jogszerűsége a munkavállalók jóváhagyásának megszerzésével biztosítható. Egy olyan esetben, amikor a munkáltató azt mondja, hogy szüksége van a hozzájárulásra, és a munkavállalót a hozzájárulás megtagadása miatt hátrány éri vagy érheti (ami munkaviszony esetén igen valószínű, különösen, amikor arról van szó, hogy a munkaadó nyomon követi az alkalmazott viselkedését), a hozzájárulás nem érvényes, hiszen megadása nem önkéntes, és nem is lehet az. A munkavállalók adatainak kezeléséhez ezért a legtöbb esetben a munkavállaló jóváhagyása nem szolgálhat és nem is szolgálhatna jogalapul, így más jogalapra van szükség.

Ezen túl még azokban az esetekben is, ahol a hozzájárulás az adatkezelés érvényes jogalapjának tekinthető (azaz kétségkívül megállapítható, hogy a hozzájárulás megadása önkéntes), a hozzájárulásnak a munkavállaló kívánságának kifejezett és tájékozott kinyilvánításának kell lennie. Az eszközök alapértelmezett beállításai és/vagy az elektronikus személyesadat-kezelés folyamatát segítő szoftverek telepítése nem tekinthető a munkavállalók által adott hozzájárulásnak, mivel a hozzájáruláshoz az akarat aktív kinyilvánítása szükséges. A cselekvés hiánya (azaz az alapértelmezett beállítások módosításának elmulasztása) sem tekinthető általánosságban az adatkezeléshez való kifejezett hozzájárulásnak[11].

- **Szerződés teljesítése (7. cikk b) pont)**

A munkaviszony gyakran a munkáltató és a munkavállaló között létrejött munkaszerződésen alapuló. Az ilyen szerződésből eredő kötelezettségek teljesítéséhez, például a munkavállaló kifizetéséhez szükséges, hogy a munkáltató bizonyos személyes adatokat kezeljen.

- **Jogi kötelezettségek (7. cikk c) pont)**

Meglehetősen gyakori, hogy a foglalkoztatási jogszabályok olyan jogi kötelezettségeket írnak elő a munkáltató számára, amelyek személyes adatok kezelését teszik szükségessé (pl. az adó kiszámításához és a munkabér kezeléséhez). Egyértelmű, hogy ilyen esetekben az adott jogszabály az adatkezelés jogalapjául szolgál.

- **Jogos érdek (7. cikk f) pont)**

Ha a munkáltató az adatvédelmi irányelv 7. cikk f) pontja szerinti jogos érdekre kíván hivatkozni, az adatkezelés céljának törvényesnek kell lennie, és az adatkezelés megvalósításához választott módszernek/technológiának a munkáltató jogos érdeke szempontjából szükségesnek kell lennie. Az adatkezelésnek emellett arányosnak is kell lennie ahhoz az üzleti igényhez, azaz a célhoz képest, amelynek érdekében alkalmazzák. A munkahelyi adatkezelést a magánszférába lehető legkevésbé behatoló módon, a kijelölt

[11] Lásd még a 29. cikk szerinti munkacsoport *15/2011. sz. véleményét a hozzájárulás definíciójáról*, WP187, 2011. július 13., url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf, 24. oldal.

kockázatra irányulóan kell kivitelezni. Ezen felül a 7. cikk f) pontjára való hivatkozás esetén a munkavállalónak megmarad az a joga, hogy a 14. cikk szerinti lényeges jogos érdekből tiltakozhasson az adatkezelés ellen.

Ahhoz, hogy valaki az adatkezelés jogalapjaként a 7. cikk f) pontjára hivatkozhasson, elengedhetetlen olyan konkrét kockázatcsökkentő intézkedések alkalmazása, amelyek célja a munkáltató jogos érdeke és a munkavállalók alapvető jogai és szabadsága közötti megfelelő egyensúly biztosítása[12]. Az ilyen intézkedéseknek a megfigyelés formájától függően magukban kell foglalniuk a megfigyelés korlátozását, ami garantálja, hogy a munkavállaló magánélet tiszteletben tartásához való joga ne sérüljön. Az ilyen korlátozások lehetnek:

- földrajzi jellegűek (pl. meghatározott helyekre korlátozódó megfigyelés; az érzékeny területek, így a vallási jellegű helyek, és például a tisztálkodó- és pihenőhelyiségek megfigyelését meg kell tiltani),
- adatalapúak (pl. a személyes elektronikus állományok és kommunikáció megfigyelése mellőzendő), továbbá
- időalapúak (pl. folyamatos megfigyelés helyett mintavétel alkalmazása).

3.1.2 *ÁTLÁTHATÓSÁG (10. ÉS 11. CIKK)*

A 10. és 11. cikk átláthatóságra vonatkozó követelményei a munkahelyen történő adatkezelésre is vonatkoznak; a munkavállalókat tájékoztatni kell a megfigyelés tényéről, a személyes adatok kezelésének céljáról, és minden egyéb információról, ami a tisztességes adatfeldolgozás garantálásához szükséges.

Az új technológiák létrejötte még egyértelműbbé teszi az átláthatóság szükségességét, mivel azok potenciálisan hatalmas mennyiségű személyes adat összegyűjtését és további feldolgozását teszik lehetővé.

3.1.3 *AUTOMATIZÁLT DÖNTÉSEK (15. CIKK)*

Az adatvédelmi irányelv 15. cikke biztosítja az érintettek jogát arra, hogy ne terjedhessen ki rájuk kizárólag automatizált adatkezelésen alapuló olyan döntés hatálya, amely rájuk nézve jogi hatással járna, vagy őket hasonlóan jelentős mértékben érintené, és amely kizárólag automatizált, egyes személyes jellemzők, például a munkahelyi teljesítmény kiértékelésére irányuló feldolgozáson alapul, kivéve, ha a döntésre szerződés megkötéséhez vagy teljesítéséhez van szükség, ha azt uniós vagy tagállami jogszabály engedélyezi, vagy az az érintett kifejezett jóváhagyásán alapul.

3.2 2016/679 rendelet — Általános adatvédelmi rendelet

Az általános adatvédelmi rendelet magában foglalja és továbbfejleszti az adatvédelmi irányelv követelményeit. Emellett új követeléseket is bevezet minden adatkezelő, így a munkáltatók számára is.

[12] Az elérendő egyensúlyra vonatkozó példáért lásd pl. a *Köpke v Németország ügyet*, [2010] EJEB, 1725. szám, (URL: http://www.bailii.org/eu/cases/ECHR/2010/1725.html), amelyben egy munkavállalót a munkáltató és egy magánnyomozó társaság által végrehajtott titkos megfigyelési művelet eredményeként elbocsátottak. Bár a bíróság azt állapította meg, hogy a nemzeti hatóságok méltányos egyensúlyt teremtettek a munkáltató (tulajdonának védelméhez fűződő) jogos érdeke és a munkavállaló magánélet tiszteletben tartásához való joga, továbbá az igazságszolgáltatáshoz fűződő közérdek között, azt is megjegyezte, hogy a technológia fejlődése következtében az ügyben szereplő különféle érdekek súlyozása a jövőben módosulhat.

3.2.1 *BEÉPÍTETT ADATVÉDELEM*

Az általános adatvédelmi rendelet 25. cikke előírja a beépített és alapértelmezett adatvédelem alkalmazását az adatkezelők számára. Például: a munkáltató által a munkavállalóknak kiadott eszközökhöz kapcsolódó nyomon követési technológiák alkalmazása esetén az adatvédelmet leginkább támogató megoldásokat kell választani. Szintén figyelemmel kell lennie az adatminimalizálásra.

3.2.2 *ADATVÉDELMI HATÁSVIZSGÁLATOK*

Az általános adatvédelmi rendelet 35. cikke rögzíti, hogy az adatkezelőnek adatvédelmi hatásvizsgálatot kell folytatnia, az adatkezelés valamely – különösen új technológiákat alkalmazó – típusa –, figyelemmel annak jellegére, hatókörére, körülményére és céljaira, valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve. Ilyen például a természetes személyekre vonatkozó egyes személyes jellemzők olyan módszeres és kiterjedt értékelése, amely automatizált adatkezelésen – ideértve a profilalkotást is – alapul, és amelyre a természetes személy tekintetében joghatással bíró vagy a természetes személyt hasonlóképpen jelentős mértékben érintő döntések épülnek.

Amint azt a munkacsoport adatvédelmi hatásvizsgálatra vonatkozó iránymutatása pontosítja[13], ha az adatvédelmi hatásvizsgálat szerint az adatkezelő nem tudja megfelelően kezelni az azonosított kockázatokat — azaz a fennmaradó kockázat továbbra is magas —, az adatkezelőnek az adatkezelés megkezdése előtt egyeztetnie kell a felügyeleti hatósággal (36. cikk (1) bek.).

3.2.2 *„Foglalkoztatással összefüggő adatkezelés”*

Az általános adatvédelmi rendelet 88. cikke rögzíti, hogy a tagállamok jogszabályban vagy kollektív szerződésekben pontosabban meghatározott szabályokat állapíthatnak meg annak érdekében, hogy biztosítsák a jogok és szabadságok védelmét a munkavállalók személyes adatainak a foglalkoztatással összefüggő kezelése tekintetében. Ilyen szabályok hozhatók különösen az alábbiakra vonatkozóan:

- munkaerő-felvétel;
- munkaszerződés teljesítése (ideértve a jogszabályban vagy kollektív szerződésben meghatározott kötelezettségek teljesítését);
- a munka irányítása, tervezése és szervezése;
- a munkahelyi egyenlőség és sokféleség;
- a munkahelyi egészségvédelmet és biztonság;
- a munkáltató vagy a vevő tulajdonának védelme;
- a foglalkoztatáshoz kapcsolódó jogok és juttatások (egyéni) gyakorlása és élvezete; valamint
- a munkaviszony megszüntetése.

A 88. cikk (2) bekezdésének megfelelően e szabályoknak olyan megfelelő és egyedi intézkedéseket kell magukban foglalniuk, amelyek alkalmasak az érintett emberi méltóságának, jogos érdekeinek és alapvető jogainak megóvására, különösen

[13] 29. cikk szerinti munkacsoport: *Iránymutatások az adatvédelmi hatásvizsgálatról és annak meghatározásáról, hogy az adatkezelés valószínűsíthetően „nagy kockázattal” jár-e a 2016/679 rendelet értelmében*, WP 248, 2017. április 4., url: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137, 18. oldal

- az adatkezelés átláthatósága;
- a személyes adatok vállalkozáscsoporton vagy a közös gazdasági tevékenységet folytató vállalkozások adott csoportján belüli továbbítása; valamint
- a munkahelyi ellenőrzési rendszerek tekintetében.

Ebben a véleményben a munkacsoport iránymutatást nyújt az új technológiák egyes konkrét helyzetekben történő jogszerű használatára, részletesen bemutatva a munkavállalók emberi méltóságának, jogos érdekeinek és alapvető jogainak védelmét szolgáló megfelelő, egyedi intézkedéseket.

4. Kockázatok

A modern technológiák lehetővé teszik a munkavállalók különböző időpontokban, különböző munkahelyeken és otthonukban történő nyomon követését számos különböző eszköz, pl. okostelefon, asztali számítógép, táblagép, jármű vagy viselhető eszköz segítségével. Ha nem szabunk határt az adatkezelésnek, és nem tesszük átláthatóvá, nagy a veszélye annak, hogy a munkáltatók hatékonyságnöveléshez és a vállalati tulajdon védelméhez fűződő jogos érdeke igazolhatatlan, a magánszférába behatoló megfigyeléssé alakul.

A kommunikáció megfigyelésére szolgáló technológiák dermesztő hatással lehetnek a munkavállalók szerveződéshez, dolgozói gyűlések szervezéséhez és bizalmas kommunikációhoz való alapvető jogai tekintetében is (beleértve az információk kereséséhez való jogot). A kommunikáció és a viselkedés megfigyelése alkalmazkodásra kényszeríti a munkavállalókat, nehogy olyasmit fedezzen fel náluk, ami rendellenesnek minősülhet - hasonlóan ahhoz, ahogyan a biztonsági kamerák használatának elterjedése is hatással van a polgárok közterületen tanúsított magatartására. Az ilyen technológiák képességeinek köszönhetően ráadásul a munkavállalók nem feltétlenül vannak tudatában annak, hogy milyen személyes adatok és milyen célból kezelnek, sőt, az is előfordulhat, hogy magának a megfigyelési technológiának a létezéséről sem tudnak.

Az információs technológiák használatának megfigyelése abban is különbözik a látható megfigyelési eszközök, például a biztonsági kamerák alkalmazásától, hogy az előbbi titokban is végezhető. Könnyen érthető, könnyen hozzáférhető munkahelyi megfigyelési szabályzat hiányában a munkavállalók esetleg nincsenek tisztában az alkalmazott megfigyeléssel és annak következményeivel, így a jogaikat sem tudják gyakorolni. További kockázatot jelent az adatok túlzott „felgyülemlése” az ilyen rendszerekben, például a wifialapú, tartózkodási helyre vonatkozó adatokat gyűjtő rendszerekben.

A munkahelyen keletkező adatok mennyiségének növekedése az új adatelemzési és adatpárosítási technikákkal ötvözve a nem összeegyeztethető további adatkezelés kockázatát is felveti. Jogszerűtlen további adatkezelés például az vagyonvédelmi célra jogszerűen üzembe helyezett rendszereknek a munkavállalók rendelkezésre állásának, teljesítményének és vevőkkel szembeni barátságosságának megfigyelésére történő felhasználása. Szintén ide tartozik a biztonsági kamerákból gyűjtött adatok felhasználása a munkavállalók viselkedésének és teljesítményének rendszeres megfigyelésére, vagy egy tartózkodási hely meghatározására szolgáló rendszer (például wifi- vagy bluetoothalapú nyomon követő rendszer) használata a munkavállalók mozgásának és magatartásának folyamatos ellenőrzésére.

Emiatt a nyomon követés sértheti a munkavállalók magánélet tiszteletben tartásához való jogát, függetlenül attól, hogy a megfigyelésre rendszeresen vagy alkalomszerűen kerül-e sor. A kockázat nem korlátozódik a közlések tartalmának elemzésére. Az egyénhez kötődő metaadatok elemzése az érintett életének és magatartási mintázatainak olyan részletes megfigyelését teszi lehetővé, ami hasonló mértékű beavatkozást jelent a magánszférába.

A megfigyelési technológiák kiterjedt használata csökkentheti a munkavállalók hajlandóságát arra, hogy értesítsék a munkáltatókat a feletteseik és/vagy más munkavállalók szabálytalan vagy törvénytelen cselekedeteiről, amelyek kárt okozhatnak a vállalkozásnak (különösen a vevőadatokban) vagy a munkahelynek (és csökkenthetik azoknak a csatornáknak a számát, amelyeken keresztül ezt egyáltalán megtehetik). Az aggódó munkavállaló számára a névtelenség gyakran feltétele annak, hogy cselekedjen, és bejelentse az ilyen helyzetet. A munkavállalók magánélet tiszteletben tartásához való jogát sértő megfigyelés gátolhatja a megfelelő tisztségviselőkkel való kommunikációt. Ebben az esetben a szervezeten belüli közérdekű bejelentések számára kialakított eszközök hatástalanná válhatnak[14].

5. Szituációk

Ebben a részben olyan munkahelyi adatkezelési szituációkat vizsgálunk, amelyek esetében az új technológiák és/vagy a meglévő technológiák továbbfejlesztése nagy kockázatot jelent vagy jelenthet a munkavállalók magánélete tekintetében. A munkáltatónak minden ilyen esetben meg kell vizsgálnia, hogy:

- az adott adatkezelési tevékenység szükséges-e, és ha igen, mi a jogalapja;
- a személyes adatok kívánt kezelése tisztességes-e a munkavállalókkal szemben;
- az adatkezelés arányos-e a felmerült problémákkal; valamint
- az adatkezelés átlátható-e.

5.1 Adatkezelés a munkaerő-felvételi folyamat során

A közösségi média használata a természetes személyek körében elterjedt, és viszonylag gyakori, hogy a felhasználói profil - a felhasználói fiók tulajdonosának beállításaitól függően - bárki számára megtekinthető. A munkáltatók ezért azt gondolhatják, hogy a jelentkezők közösségi profiljának megtekintése megengedett a toborzási folyamat során. Hasonló lehet a helyzet potenciális alkalmazottra vonatkozó egyéb, nyilvánosan elérhető információk esetében is.

A munkáltatók azonban nem feltételezhetik, hogy pusztán azért, mert valaki közösségi médiabeli profilja nyilvánosan megtekinthető, ezeket az adatokat saját céljaikra kezelhetik. Az ilyen adatkezeléshez jogalap szükséges, például a jogos érdek. Ilyen esetben a munkáltatónak a közösségi médiában létrehozott profil vizsgálata előtt figyelembe kell vennie, hogy a jelentkező profilja magán- vagy munkacélú-e, mert ez fontos szempont lehet az adatok vizsgálatának jogi elfogadhatósága tekintetében. Ezen felül a munkáltatók a jelentkezőkről csak olyan mértékben gyűjthetnek és kezelhetnek személyes adatokat, amilyen

[14] Lásd például a 29. cikk szerinti munkacsoport *1/2006. számú véleményét az Uniós adatvédelmi szabályok belső közérdekű bejelentési rendszerek tekintetében történő alkalmazásáról a számvitel, a belső számviteli ellenőrzés, a könyvvizsgálat, valamint a megvesztegetés, a banki és pénzügyi bűncselekmények elleni küzdelem terén*, WP 117, 2006. február 1., url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2006/wp117_en.pdf.

mértékben az ilyen adatok gyűjtése szükséges és releváns azon munkakör betöltése szempontjából, amelyre az illető jelentkezik.

A munkaerő-felvételi folyamat során gyűjtött adatokat általánosságban azonnal törölni kell, amint világossá válik, hogy nem tesznek ajánlatot az illető felvételre, vagy azt az illető nem fogadja el[15]. Az ilyen adatkezelésről az érintettet megfelelően tájékoztatni kell, mielőtt a munkaerő felvételi folyamatba belép.

A munkáltatónak nincs jogalapja arra, hogy a potenciális munkavállalótól megkövetelje, hogy a potenciális munkáltatót barátnak jelölje meg, vagy egyéb módon hozzáférést biztosítson számára a profilja tartalmához.

Példa

Új munkatársak felvétele során a munkáltató megtekinti a jelentkezők különböző közösségi hálózatokon található profiljait, és az ilyen hálózatokban megtalálható (valamint az interneten másutt fellelhető) információkat bevonja a szűrési folyamatba.

A munkáltató csak akkor rendelkezhet a 7. cikk f) pontja alapján jogalappal a jelentkezők nyilvánosan elérhető információinak áttekintésére, ha az adott munkakörhöz szükség van a jelentkezőről a közösségi médiában elérhető információk áttekintésére, például a jelentkező meghatározott feladattal kapcsolatos konkrét kockázatainak felmérése céljából, és csak akkor, ha jelentkezőket erről megfelelően tájékoztatják (például az álláshirdetés szövegében).

[15] Lásd még az Európa Tanács *Miniszteri Bizottságának személyes adatok foglalkoztatással összefüggő kezeléséről szóló CM/Rec(2015)5 ajánlása* 13.2 pontját (2015. április 1., url: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c3f7a). Abban az esetben, ha a munkáltató egy későbbi munkalehetőség céljára meg kívánja őrizni az adatokat, az érintettet erről értesíteni kell, és lehetőséget kell számára biztosítani az adatkezelés elleni tiltakozásra, mely esetben az adatokat törölni kell (ld. uott).

5.2 Munkaviszony során végzett megfigyelésből eredő adatfeldolgozási műveletek

A közösségi médiában létrehozott profiloknak és az új elemzési technológiák fejlődésének köszönhetően a munkáltatók olyan műszaki lehetőségekkel rendelkeznek (vagy szerezhetnek be), amelynek segítségével folyamatosan figyelhetik a munkavállalókat, információkat gyűjtve azok barátairól, véleményéről, meggyőződéséről, érdeklődési köréről, szokásairól, tartózkodási helyéről, hozzáállásról és viselkedéséről, azaz adatokat, köztük érzékeny adatokat rögzítve a munkavállaló magánéletéről és családi életéről.

A munkavállalók közösségi médiabeli profiljainak a munkaviszony során történő, általános célú figyelése nem megengedhető.

Emellett a munkáltatóknak tartózkodniuk kell attól, hogy előírják a munkavállalók vagy jelentkezők számára a hozzáférés biztosítását azokhoz az információkhoz, amelyeket közösségi hálózaton keresztül másokkal megosztanak.

Példa
A munkáltató figyeli a korábbi munkavállalók LinkedIn profilját a versenytilalmi kikötések lejártáig. A megfigyelés célja az ilyen kikötések betartásának ellenőrzése. A megfigyelés ezekre a korábbi munkavállalókra korlátozódik.

Ha a munkáltató bizonyítani tudja, hogy a megfigyelés a jogos érdekei védelméhez szükséges, és hogy annak nincsen más, a magánéletbe való kisebb beavatkozást okozó módja, valamint hogy a volt alkalmazottak megfelelő tájékoztatást kapnak a nyilvános közléseik rendszeres megfigyelésének mértékéről, a munkáltató sikerrel hivatkozhat az adatvédelmi irányelv 7. cikk f) pontjában megfogalmazott jogi alapra.

A munkavállalók számára nem írható elő a munkáltató által biztosított közösségi médiabeli profil használata. Még ha ez a feladataikra való tekintettel kifejezetten szükséges is (pl. egy szervezet szóvivője esetében), lehetőséget kell számukra biztosítani egy „nem munkahelyi", nem nyilvános profil használatára a hivatalos, munkáltatóhoz kötődő profil helyett, és ezt rögzíteni kell a munkaszerződésben.

5.3 Az információs és kommunikációs technológiák munkahelyi használatának megfigyeléséből eredő adatfeldolgozási műveletek

Hagyományosan a munkahelyi elektronikus kommunikáció (pl. telefon, internetes böngészés, elektronikus levelezés, azonnali üzenetküldés, VOPI hangkapcsolat) megfigyelését tekintették a munkavállalók magánéletét fenyegető fő veszélynek. A 29. cikk szerinti munkacsoport *az elektronikus kommunikáció munkahelyi megfigyeléséről* szóló, 2001-es *munkadokumentumban* több következtetést levont az elektronikus levelezés és az internethasználat megfigyelésére vonatkozóan. Bár e következtetések továbbra is érvényesek, figyelembe kell venni, hogy a technológia fejlődésével a megfigyelés új, a magánéletbe potenciálisan nagyobb behatolást jelentő, és még inkább mindenre kiterjedő módjai váltak lehetővé. Ilyen fejlesztések többek között a következők:

- az adatvesztés megakadályozását szolgáló (DLP) eszközök, amelyek a potenciális adatvédelmi incidensek felismerése érdekében figyelik a kimenő kommunikációt;

- az újgenerációs tűzfalak és az egyesített fenyegetéskezelő rendszerek, amelyek többféle nyomon követési technológiát kínálhatnak, köztük a következőket: csomagok mélyvizsgálata (deep packet inspection), TLS megszakítás (TLS interception), honlapszűrés, tartalomszűrés, készülékalapú adatszolgáltatás (on-appliance reporting), felhasználók kilétére vonatkozó információk, és (a fentiekben ismertetett) adatvesztés-megelőzés. Ez utóbbi technológiák külön-külön is alkalmazhatók, ha a munkáltató kívánja;
- biztonsági alkalmazások és intézkedések, amelyek rögzítik a munkavállalók bejelentkezéseit a munkáltató rendszereibe;
- eDiscovery technológia, azaz minden olyan eljárás, amely bizonyítékként felhasználni kívánt elektronikus adatok keresésére szolgál;
- az alkalmazások és eszközök használatának megfigyelése láthatatlan szoftver segítségével, akár az asztali számítógépen, akár a felhőben;
- felhőalapú szolgáltatásként nyújtott irodai alkalmazások használata a munkahelyen, melyek elméletileg a munkavállalók tevékenységének nagyon részletes naplózását teszik lehetővé;
- a munkavállalók által az erre vonatkozó felhasználási szabályzat alapján, saját munkavégzésük céljára biztosított, személyes eszközök (pl. számítógépek, mobiltelefonok, táblagépek) megfigyelése; valamint a mobileszköz-kezelési technológia, amely lehetővé teszi alkalmazások, adatok, konfigurációs beállítások és frissítések kiküldését a mobil eszközökre; valamint
- viselhető eszközök (pl. egészségügyi és fitneszkészülékek).

A munkáltató egy „minden egyben” megfigyelési megoldást is alkalmazhat, például olyan biztonsági programcsomagot, amely minden információs és kommunikációs technológia használatának megfigyelését lehetővé teszi a munkahelyen, nem csupán az elektronikus levelezését és/vagy a honlapokét, mint egykor. A WP55 dokumentumban rögzített következtetések minden olyan rendszerre érvényesek, amely ilyen megfigyelést tesz lehetővé[16].

Példa

A munkáltató TLS-ellenőrző eszközt kíván üzembe helyezni a biztonságos adatforgalom titkosításának feloldásához és ellenőrzéséhez, azzal a céllal, hogy azonosítson bármit, ami káros. Az eszköz egyben képes arra is, hogy rögzítse és elemezze a munkavállalók minden online tevékenységét, amit a szervezet hálózatán végeznek.

Egyre elterjedtebb a titkosított kommunikációs protokollok használata az személyes adatokat tartalmazó adattovábbítás lehallgatás elleni védelme érdekében. Ez azonban problémát is okozhat, hiszen a titkosítás ehetetlenné teszi a kimenő és bejövő adatok megfigyelését. A TLS-ellenőrző eszköz feloldja a továbbított adatok titkosítását, biztonsági célú ellenőrzést végez annak tartalmát, majd újra titkosítja az adatfolyamot.

[16] Lásd még: az EJEB *Copland kontra Egyesült Királyság ítéletet*, [2007], 253. szám, , (45 EHRR 37, 25 BHRC 216, 2 ALR Int'l 785, url: http://www.bailii.org/eu/cases/ECHR/2007/253.html), ahol a bíróság kimondta, hogy a vállalkozás helyiségeiből küldött elektronikus levelek és az internethasználat megfigyeléséből nyert információk a munkavállaló magánéletének és levelezésének részét képezhetik, és hogy az ilyen információk munkavállaló tudta nélküli gyűjtése és tárolása a munkavállaló jogainak megsértését jelenti, bár nem zárta ki, hogy az ilyen megfigyelés soha ne lenne szükséges egy demokratikus társadalomban.

Ebben a példában a munkáltató jogos érdekekre hivatkozik: arra, hogy meg kell védenie a hálózatot és a munkavállalók és a vevők adott hálózaton tárolt személyes adatait a jogosulatlan hozzáféréstől és az adatok kiszivárgásától. A munkavállalók valamennyi online tevékenységének megfigyelése azonban aránytalan reakció, amely sérti a közlések titkosságához való jogot. A munkáltatónak először meg kell vizsgálnia, hogy milyen, a magánéletbe való kisebb behatolást jelentő módon védheti meg a vevők adatainak titkosságát és a hálózat biztonságát.

Amennyiben a TLS-forgalom egy részének elfogása feltétlenül szükségesnek minősül, az erre szolgáló eszközt úgy kell beállítani, hogy megakadályozza a munkavállalók tevékenységének folyamatos naplózását, például úgy, hogy a gyanús bejövő vagy kimenő forgalmat blokkolja, és a felhasználót egy olyan tájékoztató portálra irányítja, ahol kérheti az automatizált döntés felülvizsgálatát. Ha az általános naplózás valamilyen formája ennek ellenére feltétlenül szükségesnek minősül, az eszköz beállítható úgy, hogy a naplózási adatokat csak akkor tárolja, ha az eszköz incidens bekövetkezését jelzi, és így a gyűjtött információk mennyisége a minimálisra csökkenjen.

Helyes gyakorlat, ha a munkáltató másik hozzáférést is biztosít a munkavállalóknak, amely nem áll megfigyelés alatt. Ez megvalósítható ingyenes vezeték nélküli internet-hozzáférés vagy különálló készülékek/terminálok biztosításával (a közlések bizalmasság biztosító, megfelelő óvintézkedések mellett), amelyeken a munkavállalók gyakorolhatják a munkahelyi eszközök bizonyos mértékű magáncélú használatához való törvényes jogukat[17]. A munkáltatónak emellett figyelemmel kell lennie arra, hogy bizonyos típusú forgalmak — mint például a magáncélú webes levelezés, az online banki funkciók használata vagy az egészségügyi honlapok felkeresése — elfogása veszélyeztetheti a munkáltató jogos érdekei és a munkavállalók magánélethez való joga közötti megfelelő egyensúlyt, hogy ennek megfontolása alapján a készüléket úgy állítsa be, hogy ne fogja el a közlést, ha a körülmények nem felelnek meg az arányosság elvének. A munkavállalókkal közölni kell, hogy a készülék a közlések milyen típusait figyeli meg.

Ki kell dolgozni egy szabályzatot arra, hogy mikor és ki férhet hozzá a gyanús naplózási adatokhoz, és ezt folyamatosan elérhetővé kell tenni valamennyi munkavállaló számára, azért is, hogy útmutatóul szolgáljon a hálózat és a létesítmények elfogadható, illetve nem elfogadható használatára vonatkozóan. Ez lehetővé teszi a munkavállalók számára, hogy viselkedésüket úgy módosítsák, hogy ne figyeljék meg őket, amikor a munkahelyi informatikai létesítményeket jogszerűen magáncélra használják. Helyes gyakorlat az ilyen szabályzat legalább éves rendszerességű kiértékelése annak meghatározásához, hogy a választott megfigyelési megoldás elérte-e a kívánt célt, és hogy van-e más, kevésbé zavaró eszköz vagy módszer ugyanazon eredmény elérésére.

Függetlenül a technológiától és annak képességeitől, a 7. cikk f) pontjában foglalt jogalap csak akkor alkalmazható, ha az adatfeldolgozás bizonyos feltételeknek megfelel. Az ilyen termékeket és alkalmazásokat használó munkáltatóknak elsőként az alkalmazott intézkedések

[17] Lásd: az EJEB *Halford kontra Egyesült Királyság ítéletet*, [1997] 32. szám, (url: http://www.bailii.org/eu/cases/ECHR/1997/32.html), ahol a bíróság kimondta, hogy „a vállalat helyiségeiből és az otthonról indított hívások egyaránt beletartozhatnak a „magánélet" és a „levelezés" 8. cikk 1. bekezdése szerinti fogalmába [az Egyezmény szerint]"; valamint az EJEB *Barbulescu kontra Románia* ítéletet, [2016] 61. szám, (url: http://www.bailii.org/eu/cases/ECHR/2016/61.html), amelyben egy professzionális üzenetküldési felhasználói fiók személyes célú felhasználása tekintetében a bíróság megállapította, hogy a felhasználói fiók munkáltató általi megfigyelése korlátozott mértékű és megfelelő volt; valamint Pinto de Alberquerque bíró különvéleményét, amelyben a megfontolt egyensúly megteremtése mellett érvel.

arányosságát kell megvizsgálniuk, és azt, hogy tehetnek-e további lépéseket az adatkezelés mértékének és hatásának mérséklésére vagy csökkentésére. Helyes gyakorlat, ha ennek felmérésére egy adatvédelmi hatásvizsgálat keretében kerül sor, még mielőtt bármilyen megfigyelési technológia bevezetésre kerül. Emellett a munkáltatóknak az adatvédelmi szabályzat mellett az elfogadható használatra vonatkozó szabályzatot is be kell vezetniük és közzé kell tenniük, amelyben meghatározzák a szervezet hálózatának és berendezéseinek megengedett használatát, és részletesen ismertetik az alkalmazott adatkezelést.

Egyes országokban egy ilyen szabályzat létrehozásához az üzemi tanács vagy más munkavállalói érdekképviseleti szerv jóváhagyása szükséges. A gyakorlatban az ilyen szabályzatokat gyakran az informatikai eszközök karbantartásával foglalkozó munkatársak fogalmazzák meg. Mivel ők elsősorban a biztonságra összpontosítanak, nem a munkavállalók magánélettel kapcsolatos jogos elvárásaira, a munkacsoport javasolja, hogy minden esetben vonják be a munkavállalók egy reprezentatív mintáját a megfigyelés szükségességének, valamint a szabályzat logikájának és hozzáférhetőségének értékelésébe.

Példa

A munkáltató adatvesztés megelőzésére szolgáló eszközt helyez üzembe, amely automatikusan figyeli a kimenő elektronikus leveleket, hogy megakadályozza a jogvédett adatok (például vevők személyes adatai) jogosulatlan továbbítását, függetlenül attól, hogy ez szándékosan vagy nem szándékosan történik-e. Amennyiben egy elektronikus levél adatvédelmi incidens potenciális forrásának minősül, további vizsgálatra kerül sor.

A munkáltató itt is a jogos érdekre hivatkozik, amennyiben védenie kell a vevők személyes adatait és saját tulajdonát a jogosulatlan hozzáféréstől és az adatok kiszivárgásától. A DLP eszköz használata azonban a személyes adatok felesleges kezelésével járhat, például egy hamis pozitív riasztás a munkavállaló által küldött, jogszerű elektronikus levelekhez (adott esetben személyes levelekhez) való jogosulatlan hozzáférést eredményezhet.

A DLP eszköz szükségességének és használatának ezért teljes mértékben indokoltnak kell lennie, hogy megfelelő egyensúly álljon fel a munkáltató jogos érdekei és a munkavállalók személyes adatok védelméhez fűződő alapvető jogai között. Ahhoz, hogy a munkáltató jogos érdekre hivatkozhasson, bizonyos intézkedéseket kell tennie a kockázatok csökkentésére. Például azoknak a szabályoknak, amelyek alapján a rendszer potenciális adatvédelmi incidensnek minősít egy elektronikus levelet, teljes mértékben átláthatónak kell lenniük a felhasználók számára, és amennyiben az eszköz egy elküldés előtt álló elektronikus levelet potenciális adatvédelmi incidensnek minősít, az elküldés előtt erről figyelmeztető üzenetben kell tájékoztatni a feladót, hogy lehetősége legyen az elküldés megakadályozására.

Bizonyos esetekben a munkavállalók megfigyelését nem is annyira meghatározott technológiák alkalmazása teszi lehetővé, hanem az az elvárás, hogy a munkavállalók a munkáltató által rendelkezésre bocsátott, személyes adatokat kezelő online alkalmazásokat használjanak. Példa erre a felhőalapú irodai alkalmazások (pl. szövegszerkesztő programok, naptárak, közösségi networking megoldások) használata. Biztosítani kell, hogy a munkavállalók kijelölhessenek olyan magáncélú tereket, amelyekhez a munkáltató csak kivételes körülmények között férhet hozzá. Ez szükséges például a naptárak esetében, amelyeket gyakran használnak magánjellegű időpontok rögzítésére is. Ha a munkavállaló egy adott időpontot magánjellegűként jelölt meg, vagy ezt magában az időpontbejegyzésben jelezte, biztosítani kell, hogy a munkáltató (és más munkavállalók) ne tekinthessék meg az időpontbejegyzés tartalmát.

A szubszidiaritás követelménye e téren néha azt jelenti, hogy semmilyen megfigyelés nem végezhető. Ez a helyzet áll fenn például akkor, ha a kommunikációs szolgáltatások tiltott használata megakadályozható bizonyos honlapok elérhetetlenné tételével. Ha a kommunikáció folyamatos megfigyelése helyett lehetőség van a honlapok elérhetetlenné tételére, a szubszidiaritás követelményének betartása érdekében az utóbbit kell választani.

Általánosságban is igaz, hogy sokkal nagyobb súlyt kell helyezni a megelőzésre, mint a felderítésre: a munkáltató érdekét jobban szolgálja az internet nem megfelelő használatának műszaki eszközökkel történő megelőzése, mint ha erőforrásait a visszaélés felderítésére kell fordítania.

5.4 Az információs és kommunikációs technológiák munkahelyen kívüli használatának megfigyeléséből eredő adatfeldolgozási műveletek

Az otthoni munkavégzés, a távoli munkavégzés és a saját eszközök munkacélú használatának terjedésével az információs és kommunikációs technológiák munkahelyen kívüli használata is elterjedtebbé vált. Az ilyen technológiák képességei kockázatot jelenthetnek a munkavállalók magánélete szempontjából, mivel az ilyen eszközök használata során sok esetben a munkahelyen alkalmazott megfigyelési rendszerek a munkavállaló otthoni szférájára is kiterjednek.

5.4.1 *OTTHONI ÉS TÁVOLI MUNKAVÉGZÉS MEGFIGYELÉSE*

Egyre gyakoribb, hogy a munkáltató lehetővé teszi a munkavállalók számára a távoli, például otthoni és/vagy utazás közbeni munkavégzést. Valójában ez a központi tényező amögött, hogy csökken a munkahely és az otthon közötti különbség. Ez általában azzal jár, hogy a munkáltató IKT-berendezést vagy szoftvert bocsát a munkavállaló rendelkezésére, amelyet az otthonában, illetve saját eszközére kell telepíteni, és amely azt követően - a kialakítástól függően - ugyanolyan szintű hozzáférést biztosít a számára a munkáltató hálózatához, rendszereihez és erőforrásaihoz, mintha a munkahelyén lenne.

Amellett, hogy az otthonról történő munkavégzés pozitív változás lehet, egyben új kockázatot is jelenthet a munkáltató számára. Azok a munkavállalók például, akik távoli hozzáféréssel rendelkeznek a munkáltató infrastruktúrájához, nem tartoznak ugyanazon fizikai biztonsági intézkedések hatálya alá, mint amelyek a munkáltató létesítményében érvényben vannak. Egyszerűen szólva: megfelelő műszaki intézkedések nélkül megnő a jogosulatlan hozzáférés kockázata, ami információk, köztük a munkavállalók és vevők munkáltató birtokában lévő személyes adatai elvesztéséhez vagy megsemmisüléséhez vezethet.

A munkáltató úgy vélheti, hogy az ilyen típusú kockázat mérséklése indokolhatja olyan szoftvercsomag alkalmazását (akár a fizikai helyiségekben, akár a felhőben), amely képes például a billentyűzetleütések és az egérmozgások rögzítésére, képernyőképek készítésére (akár véletlenszerűen, akár meghatározott időközönként), a használt alkalmazások (és használatuk időtartama) rögzítésére, valamint a megfelelő eszközökön a webkamerák bekapcsolására az onnan származó felvételek gyűjtésére. Az ilyen technológiák széles körben elérhetők, például külső felektől, köztük felhőalapú szolgáltatóktól.

Az ezek alkalmazásával járó adatkezelés azonban aránytalan, és igen valószínűtlen, hogy a jogos érdek jogalapként szolgálhat a munkáltató számára például egy munkavállaló billentyűzetleütéseinek és egérmozgásainak rögzítésére.

A lényeg, hogy az otthoni és a távoli munkavégzés jelentette kockázat kezelése arányos, nem eltúlzott módon történjen, függetlenül az opció felajánlásának módjától és a javasolt technológiától, különösen, ha a vállalati és a magánszféra közötti határok elmosódnak.

5.4.2 *SAJÁT ESZKÖZ MUNKACÉLÚ HASZNÁLATA*

Az elektronikus fogyasztási cikkek népszerűségének növekedésével a munkáltatókra nyomás nehezedhet a munkavállalók részéről, hogy használhassák saját eszközeiket a munkahelyen történő munkavégzéshez. Ezt értjük saját eszköz munkacélú használata alatt.

Az ezt lehetővé tévő rendszer hatékony megvalósítása számos pozitívumhoz, többek között a munkával való elégedettség növekedéséhez, az általános munkahelyi hangulat javulásához, a munka hatékonyságának növekedéséhez és nagyobb rugalmassághoz vezethet a munkavállalók körében. A dolog jellegénél fogva azonban a munkavállaló az eszközét az idő

egy részében – különösen bizonyos napszakokban, például esténként és a hétvégéken – személyes célokra használja. Ezért határozottan fennáll a lehetősége annak, hogy amennyiben a munkavállaló a saját eszközét használja, a munkáltató az adott munkavállalóra – és esetleg az adott eszközt szintén használó családtagjaikra – vonatkozó nem vállalati információkat is kezelni fog.

Munkaviszony esetén a saját eszközök munkacélú használatával kapcsolatos adatvédelmi kockázatok gyakran az azonosítókat, például MAC-címeket gyűjtő megfigyelési technológiákkal, illetve azokkal az esetekkel függenek össze, ahol a munkáltató biztonsági átvizsgálás, például káros programok keresése címén fér hozzá a munkavállaló eszközéhez. Ez utóbbi célra több kereskedelmi megoldás létezik, amely lehetővé teszi a magántulajdonú eszközök ellenőrzését, mivel azonban ezek használata az adott készüléken lévő összes adathoz való hozzáférést jelenthet, körültekintő kezelést igényelnek. Elméletileg például nem szabad hozzáférni az eszköz azon részeihez, amelyek feltételezhetően csak magáncélra szolgálnak (mint pl. a készülékkel készített fényképek tárolására szolgáló mappa).

Az ilyen eszközök tartózkodási helyének és forgalmának megfigyelésen jogos érdekeket szolgálónak minősülhet, amely jogos érdek azon személyes adatok védelme, amelyekért a munkáltató adatkezelőként felelős; a munkavállaló személyes eszközei esetében azonban az ilyen megfigyelés jogszerűtlen lehet, ha a munkavállaló magánéletéhez és családi életéhez kötődő adatokra is kiterjed. A magánjellegű információk megfigyelésének elkerülése érdekében megfelelő intézkedésekkel kell különbséget tenni az eszköz magán- és munkacélú használata között.

Emellett a munkáltatónak olyan módszereket kell alkalmaznia, amely biztosítja a készüléken lévő saját adatainak biztonságos továbbítását a készülék és a saját hálózata között. Ez történhet például úgy, hogy a biztonság meghatározott szintjének biztosítása érdekében a készülék a teljes forgalmat egy virtuális magánhálózat segítségével a vállalati hálózaton keresztül bonyolítja le; ilyen intézkedés alkalmazása esetén azonban a munkáltatónak figyelembe kell vennie, hogy a megfigyelési céllal telepített szoftverek kockázatot jelentenek a magánélet védelme tekintetében azokban az időszakokban, amikor a munkavállaló az eszközt magáncélra használja. Megfelelő lehet olyan eszközök használata, amelyek kiegészítő védelmet, például az adatok számára kialakított „homokozót” biztosítanak (azaz az adatokat egy adott alkalmazáson belül tartják).

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

5.4.3 *MOBIL ESZKÖZÖK KEZELÉSE*

A mobil eszközök kezelésére szolgáló megoldások lehetővé teszik a munkáltatók számára, hogy bármikor, távolról meghatározzák az eszközök tartózkodási helyét, adott beállításokat és/vagy alkalmazásokat telepítsenek, valamint adatokat töröljenek. A munkáltató ezeket a funkciókat használhatja saját maga, vagy azzal harmadik felet is megbízhat. Az ilyen szolgáltatások arra is lehetőséget biztosítanak, hogy a munkáltató valós időben rögzítse vagy nyomon kövesse a készüléket, akkor is, ha nem jelentették annak ellopását.

Az ilyen célú új, illetve az adatkezelő számára új technológia alkalmazása előtt adatvédelmi hatásvizsgálatot kell végezni. Ha a hatásvizsgálat azt állapítja meg, hogy a mobileszköz-

kezelési technológia meghatározott körülmények esetén szükséges, akkor is meg kell vizsgálni, hogy az ebből eredő adatkezelés megfelel-e az arányosság és a szubszidiaritás elvének. A munkáltatónak gondoskodnia kell arról, hogy a távolról történő helymeghatározás keretében gyűjtött adatok kezelése meghatározott célból történjen, és ne legyen, és ne is lehessen része egy szélesebb körű, a munkavállalók folyamatos megfigyelését lehetővé tévő programnak. Még a meghatározott célt szolgáló nyomon követés esetén is mérsékelni kell az ezzel okozott zavarás mértékét. A nyomon követést biztosító rendszer kialakítható úgy, hogy a tartózkodási helyre vonatkozó adatokat anélkül rögzítse, hogy azokat a munkáltató számára ismertté teszi – ebben az esetben a helymeghatározási adatokat csak akkor kell elérhetővé tenni, ha a készüléket bejelentik vagy elveszítik.

Azokat a munkavállalókat, akiknek eszközei bekerülnek a mobileszköz-kezelési programba, teljes körűen tájékoztatni kell az alkalmazott megfigyelésről, és arról, hogy ez milyen következményekkel jár rájuk nézve.

5.4.4 *VISELHETŐ ESZKÖZÖK*

Egyre nagyobb a kísértés a munkáltatók számára, hogy viselhető eszközöket biztosítsanak munkavállalóik számára, amelyek segítségével nyomon követhetik egészségi állapotukat és tevékenységüket a munkahelyen, sőt, néha azon kívül is. Az ilyen adatkezelés azonban egészségügyi adatokra is kiterjed, így az adatvédelmi irányelv 8. cikke értelmében tilos.

A munkáltatók és a munkavállalók között fennálló egyenlőtlen viszonyra – azaz hogy a munkavállaló anyagilag függ a munkáltatótól –, valamint az egészségügyi adatok érzékeny jellegére való tekintettel nagyon valószínűtlen, hogy jogilag érvényes kifejezett hozzájárulás adható az ilyen adatok nyomon követéséhez és megfigyeléséhez mivel a munkavállalók lényegében nem tudnak erre vonatkozó önkéntes hozzájárulást adni. Az ilyen adatkezelés még akkor is jogszerűtlen, ha a munkáltató harmadik felet bíz meg az egészségügyi adatok gyűjtésével, amely csak összesített információkat bocsát a munkáltató rendelkezésére az egészségügyi jellegű változásokról.

Emellett, amint azt az *anonimizálási technikákról szóló 5/2014. számú vélemény*[18] ismerteti, az adatok teljes anonimizálása technikailag igen nehezen megoldható. Még ha ezernél több munkavállalóról is van szó, a munkáltató számára a munkavállalókról rendelkezésére álló egyéb adatok lehetővé teszik a különböző egészségügyi problémákkal, például magas vérnyomással vagy elhízással küzdő munkavállalók egyedi azonosítását.

Példa:

A szervezet általános ajándékként fitneszmonitorozó készüléket kínál a munkavállalóinak. A készülék számlálja a munkavállaló által megtett lépéseket, valamint rögzíti a szívverését és alvási jellemzőit.

Biztosítani kell, hogy az így létrejövő egészségügyi adatokhoz csak a munkavállaló férhessen hozzá, a munkáltató ne. A munkavállaló (mint érintett) és a készülék/szolgáltatás nyújtója (mint adatkezelő) közötti esetleges adatátvitel minden esetben csak e két félre tartozik.

[18] A 29. cikk szerinti munkacsoport *5/2014. sz. véleménye az anonimizálási technikákról*, WP 216, 2014. április 10., url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

Miután az egészségügyi adatokat a készülék gyártója vagy a munkáltatóknak kínált szolgáltatások nyújtója is kezelheti, a készülék vagy szolgáltatás kiválasztásakor a munkáltatóak értékelnie kell a gyártó/szolgáltató adatvédelmi politikáját annak biztosítására, az ne eredményezhesse a munkavállalók egészségügyi adatainak jogszerűtlen kezelését.

5.5 Munkaidővel és jelenléttel kapcsolatos adatkezelési műveletek

Azok a rendszerek, amelyek a munkáltatók számára lehetővé teszik a létesítményeikbe és/vagy azon belül meghatározott területekre történő belépés ellenőrzését, a munkavállalók tevékenységének nyomon követésére is lehetőséget biztosíthatnak. Bár ilyen rendszerek már évek óta léteznek, egyre inkább terjed a munkavállalók munkaidejének és jelenlétének nyomon követését szolgáló – köztük a biometrikus adatokat kezelő, vagy éppen a mobil eszközöket nyomon követő – új technológiák alkalmazása.

Bár egy ilyen rendszer a munkáltató ellenőrzési nyomvonalának fontos eleme lehet, fennáll annak a veszélye, hogy a magánélet szempontjából zavaró mértékű ismeretet és ellenőrzési lehetőséget tesz lehetővé a munkavállaló munkahelyen folytatott tevékenysége tekintetében.

Példa:

A munkáltató szervertermet üzemeltet, ahol a vállalkozás szempontjából érzékeny adatokat, valamint a munkavállalókhoz és a vevőkhöz kapcsolódó személyes adatokat tárolnak digitális formában. Az adatok jogosulatlan hozzáférés elleni védelmére vonatkozó jogi kötelezettsége teljesítése céljából a munkáltató olyan beléptető rendszert helyezett üzembe, amely rögzíti a terembe való belépési jogosultsággal rendelkező alkalmazottak be- és kilépését. Amennyiben bármely berendezés eltűnik vagy valamely adathoz jogosulatlanul hozzáférnek, elvész vagy ellopják, a munkáltató által vezetett nyilvántartás lehetővé teszi annak megállapítását, hogy az adott időben ki fért hozzá a teremhez.

Mivel az adatkezelés szükséges, és a nem élvez előnyt a munkavállalók magánélethez való jogával szemben, a 7. cikk f) pontja szerinti jogos érdek alá eshet, feltéve, hogy a munkavállalókat megfelelően tájékoztatták az adatkezelésről. A munkavállalók pontos belépési és kilépési idejének, illetve a belépések gyakoriságának folyamatos megfigyelése azonban nem lehet indokolt, amennyiben azt más célra, például a munkavállalók teljesítményének értékelésére is használják.

5.6 Videomegfigyelési rendszer segítségével végzett adatkezelési műveletek

A videomegfigyelés és -felügyelet továbbra is a korábbiakhoz hasonló problémákat vet fel a munkavállalók magánélete szempontjából: a dolgozó magatartásának folyamatos rögzítésére való képességet[19]. A munkaviszonnyal összefüggésben alkalmazott ilyen technológiákkal kapcsolatos legfontosabb változás az összegyűjtött adatokhoz való távoli hozzáférés leegyszerűsödése (pl. okostelefonon keresztül); a kamerák méretének csökkenése (és műszaki jellemzőik javulása, pl. a HD felbontás); valamint az új videoelemző eszközök által kínált feldolgozási lehetőségek.

[19] Lásd a fent hivatkozott *Köpke kontra Németország* ügyet; meg kell továbbá jegyezni, hogy egyes országokban a zárt láncú videokamera-rendszerek és hasonló rendszerek jogszerűtlen magatartás bizonyítása céljából történő üzembe helyezését jogszerűnek minősítették; lásd a spanyol alkotmánybíróság előtt folytatott *Bershka* ügyet.

A videofelvételek elemzésére szolgáló eszközök műszaki lehetőségeinek köszönhetően a munkáltató számára lehetővé válik a dolgozó arckifejezésének automatizált megfigyelése, az előre meghatározott mozgásmintázatoktól való eltérés felismerése (pl. üzemi környezetben), és hasonlók. Ez azonban a munkavállalók jogaihoz és szabadságaihoz viszonyítva aránytalan, és így általában jogszerűtlen lenne. Az adatkezelés emellett valószínűleg profilkészítést és esetleg automatizált döntéshozatalt is magában foglalna, ezért a munkáltatóknak tartózkodniuk kell az arcfelismerési technológiák alkalmazásától. A szabály alól lehetnek speciális kivételek, de az ilyen helyzetek nem használhatók fel annak alátámasztására, hogy az ilyen technológia általános alkalmazása jogszerű[20].

5.7 A munkavállalók által használt járműveket érintő adatkezelési műveletek

Széles körben elterjedtté váltak azok a technológiák, amelyek lehetővé teszik a munkáltatók számára a járműveik megfigyelését – különösen a szállítással foglalkozó, illetve jelentős méretű járműflottával rendelkező szervezetek körében.

A járművekhez kapcsolódó telematikai eszközöket alkalmazó munkáltatók minden esetben a járműről és az adott járművet használó munkavállalóról egyaránt gyűjtenek adatot. Ezek az adatok nem csak az alapvető GPS-nyomkövető rendszerek által gyűjtött, a jármű (és így a munkavállaló) tartózkodási helyét megadó adatokat tartalmazhatják, hanem a technológia függvényében számos más, például a járművezetési szokásokra vonatkozó információkat is. Bizonyos technológiák (pl. például az eseményrögzítők) a jármű és a járművezető folyamatos megfigyelését is lehetővé teszik.

Előfordulhat, hogy a munkáltatónak azért kell nyomkövető technológiát beszereltetnie a járművekbe, hogy eleget tegyen más jogi kötelezettségeknek, például hogy biztosítsa a járművet vezető munkavállaló biztonságát. Jogos érdeke fűződhet ahhoz is, hogy bármikor meg tudja állapítani a jármű tartózkodási helyét. Még ha azonban a munkáltatónak jogos érdeke fűződik is e célokhoz, elsőként azt kell megvizsgálni, hogy az adatkezelésre szükség van-e azok eléréséhez, és hogy a tényleges megvalósítás eleget tesz-e az arányosság és a szubszidiaritás elvének. Ahol a munkavégzéshez használt jármű magáncélú használata is megengedett, a legfontosabb intézkedés, amelyet a munkáltató az említett elveknek való megfelelés érdekében tehet, az, ha lehetőséget nyújt a megfigyelés elutasítására: elméletileg a munkavállalónak lehetőséget kell biztosítani arra, hogy ideiglenesen kikapcsolja a tartózkodási hely nyomon követését, ha azt különleges körülmény, például egy orvos felkeresése indokolja. Ilyen módon a munkavállaló saját döntése alapján védetté tehet bizonyos tartózkodási helyre vonatkozó, magánjellegű adatokat. A munkáltatónak gondoskodnia kell arról, hogy az összegyűjtött adatokat ne használják jogszerűtlen további adatkezeléshez, például a munkavállalók nyomon követéséhez vagy értékeléséhez.

Emellett a munkáltatónak egyértelműen tájékoztatnia kell a munkavállalókat a nyomkövető berendezés beszereléséről az általuk vezetett vállalati járműbe, és hogy amíg az adott járművet használják, addig rögzítik a mozgásukat (valamint az alkalmazott technológiától függően esetleg a vezetési szokásaikat is). Ezeket az információkat lehetőleg jól láthatóan ki kell helyezni mindegyik autóba, a járművezető által látható helyre.

A járművek használatára vonatkozó konkrét szabályzatoktól függően előfordulhat, hogy a munkavállalók munkaidőn kívül is használják a vállalati járműveket, például magáncélra. A

[20] Az általános adatvédelmi rendelet előírja továbbá, hogy a biometrikus adatok azonosítási célú felhasználása csak a 9. cikk (2) bekezdésében foglalt kivétel alapján megengedett.

tartózkodási helyre vonatkozó adatok érzékenységére való tekintettel valószínűtlen, hogy lenne jogalap a munkáltató járművei tartózkodási helyének megfigyelésére a megállapodás szerinti munkaidőn kívül. Amennyiben ez mégis szükséges, a megvalósítás módjának a kockázattal arányosnak kell lennie. Ez például jelentheti azt, hogy az autó ellopásának megakadályozása érdekében az autó tartózkodási helyét munkaidőn kívül csak akkor rögzítik, ha a jármű elhagy egy tágan meghatározott kört (egy régiót vagy akár az országot). Emellett a tartózkodási helynek csak vészhelyzet esetén szabad láthatóvá válnia: a munkáltató a rendszerben már rögzített adatokhoz hozzáférve csak akkor aktiválhatja a tartózkodási hely megjelenítését, ha a jármű elhagyja az előre meghatározott régiót.

Amint azt a 29. cikk szerinti munkacsoport *mobil okoseszközökön alkalmazott helymeghatározási szolgáltatásokról szóló 13/2011. számú véleménye*[21] rögzíti:

> „A járműkövető eszközök nem a munkatársak követésére szolgálnak. Arra valók, hogy nyomon kövessék vagy megfigyeljék annak a járműnek a tartózkodási helyét, amelybe beszerelték őket. A munkáltatók nem tekinthetik őket olyan eszköznek, amely a járművezető vagy más munkatársak viselkedése vagy holléte nyomon követésére vagy megfigyelésére szolgál, például azzal, hogy a jármű sebességére vonatkozó figyelmeztetéseket küld."

Továbbá, amint azt a 29. cikk szerinti munkacsoport *helymeghatározási adatok értéknövelt szolgáltatások céljára történő felhasználásáról szóló 5/2005. számú véleménye*[22] kimondja:

> „A tartózkodási helyre vonatkozó adatok kezelése indokolt lehet, amikor az a személy- vagy áruszállítás megfigyelésének keretében vagy az erőforrások szétszórt helyszíneken nyújtott szolgáltatások között végzett szétosztásának tökéletesítése céljából történik (pl. valós idejű tervezés), vagy amikor a cél a munkavállaló vagy a rábízott áruk vagy járművek biztonságával kapcsolatos. A munkacsoport ezzel szemben túlzott mértékűnek ítéli az adatkezelést, ha a munkavállalók szabadon szervezhetik meg az utazásaikat, vagy ha annak kizárólagos célja a munkavállaló munkavégzésének megfigyelése, amennyiben a megfigyelés más módon is megvalósítható."

5.7.1 ESEMÉNYRÖGZÍTŐ BERENDEZÉSEK

Az eseményrögzítő berendezések a vállalati járműveket vezető munkavállalók jelentős mennyiségű személyes adatainak kezelését teszik műszakilag lehetővé a munkáltató számára. Egyre többször szerelnek fel ilyen berendezéseket járművekben azzal a céllal, hogy baleset esetén videofelvételt, esetleg hangfelvételt is készítsenek. Az ilyen rendszerek képesek meghatározott időpontban, például hirtelen fékezéskor, hirtelen irányváltáskor vagy baleset bekövetkezésekor felvételt készíteni és az incidenst közvetlenül megelőző pillanatokat eltárolni, de folyamatos megfigyelésre is beállíthatók. Az így kapott információk alapján később megfigyelhetők és áttekinthetők az adott személy vezetési szokásai, azok tökéletesítése céljából. Sok ilyen rendszer emellett GPS-funkciót is tartalmaz, amellyel valós időben követhető a jármű tartózkodási helye, és képes a járművezetéssel kapcsolatos egyéb adatok (például a jármű sebessége) eltárolására későbbi feldolgozás céljából.

[21] A 29. cikk szerinti munkacsoport *13/2011. számú véleménye a mobil okoseszközökön alkalmazott helymeghatározási szolgáltatásokról*, WP 185, 2011. május 16., url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp185_en.pdf

[22] A 29. cikk szerinti munkacsoport *5/2005. számú véleménye a helymeghatározási adatok értéknövelt szolgáltatások céljára történő felhasználásáról,* WP 115, 2005. november 25., url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2005/wp115_en.pdf

Különösen széles körben elterjedtek az ilyen berendezések a szállítással foglalkozó, illetve a jelentős méretű járműflottával rendelkező szervezetek körében. Az eseményrögzítő berendezések alkalmazása azonban csak akkor jogszerű, ha az általuk nyújtott, a munkavállalóra vonatkozó személyes adatok kezelése törvényes célból szükséges, és az adatkezelés megfelel az arányosság és a szubszidiaritás elvének.

Példa

Egy fuvarozó vállalat valamennyi járművének vezetőfülkéjébe videokamerát szerel, amely hangot és videót rögzít. Az adatkezelés célja a munkavállalók járművezetési készségeinek javítása. A kamerákat úgy állították be, hogy bármilyen incidens, például hirtelen fékezés vagy irányváltás esetén megőrizzék a felvételt. A vállalat feltételezi, hogy az irányelv 7. cikk f) pontjában foglalt jogos érdekre hivatkozva jogalappal rendelkezik az adatkezeléshez annak érdekében, hogy védje a munkavállalói és más járművezető biztonságát.

A vállalat járművezetők megfigyeléséhez fűződő jogos érdeke azonban nem élvez elsőbbséget az adott járművezetők személyes adatok védelméhez fűződő jogaival szemben. A munkavállalóknak az említett kamerával történő, folyamatos megfigyelése súlyosan sérti a magánélet tiszteletben tartásához való jogukat. Léteznek más módszerek (pl. a mobiltelefon-használatot megakadályozó berendezés beépítésre), valamint a balesetek megelőzésére szolgáló más biztonsági rendszerek (pl. a továbbfejlesztett vészfékrendszer vagy a sávelhagyásra figyelmeztető rendszer), amelyek használata megfelelőbb lehet. Az ilyen videofelvétel emellett nagy valószínűséggel harmadik felek (pl. gyalogosok) személyes adatainak kezelésével is jár, amihez a vállalat jogos érdeke nem biztosít elegendő megalapozottságot.

5.8 Munkavállalók adatainak harmadik fél részére történő átadásával járó adatkezelési műveletek

Egyre gyakoribb, hogy a vállalatok munkavállalóik adatait a szolgáltatásnyújtás biztonsága érdekében átadják a vevőiknek. A nyújtott szolgáltatások tartalmától függően ezek az adatok meglehetősen széles körűek lehetnek (pl. köztük lehet a munkavállaló fényképe). Az egyenlőtlen hatalmi viszonyok következtében azonban a munkavállalók nincsenek abban a helyzetben, hogy önkéntesen hozzájárulhassanak a személyes adataik munkáltató általi kezeléséhez, és ha az adatkezelés nem arányos, a munkáltató nem rendelkezik jogalappal.

Példa:

Egy csomagszállító vállalat elektronikus levélben linket küld a vevőknek a kiszállító személy (munkavállaló) nevéhez és tartózkodási helyéhez. A vállalat a kiszállító útlevélfényképét is ki szerette volna küldeni. A vállalat feltételezte, hogy jogos érdeke (irányelv 7. cikk f) pont) jogalapot biztosít számára az adatkezeléshez annak érdekében, hogy a lehetővé tegye a vevő számára annak ellenőrzését, hogy a kiszállító a megfelelő személy-e.

A kiszállító nevének és fényképének vevőkkel való közlése azonban nem szükséges. Mivel az ismertetett adatkezelésnek más jogszerű alapja nincs, a csomagszállító vállalkozás nem adhatja át ezeket a személyes adatokat a vevőknek.

5.9 Személyügyi adatok és más munkavállalói adatok nemzetközi továbbításával járó adatkezelési műveletek

A munkáltatók egyre gyakrabban használnak felhőalapú alkalmazásokat és szolgáltatásokat, például a személyügyi adatok kezelésére szolgáló, valamint online irodai alkalmazásokat. A legtöbb ilyen alkalmazás használata a munkavállalóktól származó, illetve rájuk vonatkozó adatok nemzetközi továbbításával jár. Amint az a 08/2001. számú vélemény már rögzítette, az irányelv 25. cikke előírja, hogy személyes adatok csak akkor továbbíthatók az Unión kívüli harmadik országba, ha az adott ország megfelelő védelmi szintet tud biztosítani. Az adattovábbításnak a jogalaptól függetlenül meg kell felelnie az irányelv rendelkezéseinek.

Ennek megfelelően biztosítani kell, hogy az adatok nemzetközi továbbítására vonatkozó fenti rendelkezések teljesüljenek. A munkacsoport megismétli azt az álláspontját, hogy előnyben kell részesíteni a megfelelő védelemre való támaszkodást az adatvédelmi irányelv 26. cikkében felsorolt eltérésekkel szemben; a hozzájárulásra való támaszkodás esetén pedig annak kifejezettnek, egyértelműnek és önkéntesnek kell lennie. Biztosítani kell azonban azt is, hogy az adatok Unión/EGT-n kívüli megosztása, valamint azt követően a csoporthoz tartozó más felek általi hozzáférés továbbra is az adott célhoz szükséges legkisebb mértékűre korlátozódjon.

6. Következtetések és ajánlások

6.1 Alapvető jogok

A fenti közlések tartalmára és az ilyen közlések forgalmi adataira ugyanúgy vonatkozik az alapvető jogok védelme, mint az „analóg” közlésekre.

A vállalat helyiségeiből folytatott elektronikus kommunikáció beletartozhat a „magánélet” és „levelezés” az emberi jogok európai egyezménye 8. cikke 1. bekezdésének értelmében vett fogalmába. A jelenlegi adatvédelmi irányelv alapján a munkáltató adatgyűjtést csak törvényes célból folytathat, az adatkezelésnek megfelelő feltételek mellett kell történnie (pl. arányosnak és szükségesnek, valós és aktuális érdeket szolgálónak kell lennie, és törvényes, részletezett és átlátható módon kell megvalósulnia), és az elektronikus kommunikációból gyűjtött vagy azzal létrehozott személyes adatok kezeléséhez jogalappal kell rendelkezni.

Az, hogy az elektronikus eszközök a munkáltató tulajdonát képezik, nem zárja ki a munkavállalók jogát a közlés titkosságához, a kapcsolódó, tartózkodási helyre vonatkozó adatok titkosságához, valamint a levéltitokhoz. A munkavállalók saját tulajdonú vagy a vállalat által kiadott eszközökön keresztül történő nyomon követésének azokra az esetekre kell korlátozódnia, ahol az valamilyen törvényes célból feltétlenül szükséges. A saját eszköz munkacélú használata esetén mindenképpen fontos, hogy a munkavállalónak lehetősége legyen magánjellegű közléseit megvédeni a munkavégzéssel kapcsolatos megfigyeléstől.

6.2 Hozzájárulás; jogos érdek

A munkavállalók a munkáltató és a munkavállalók közötti függőségi viszonyból eredően szinte soha nincsenek abban a helyzetben, hogy a hozzájárulásukat szabadon adják meg, tagadják meg vagy vonják vissza. Az erőviszonyok egyenlőtlensége miatt a munkavállalók csak kivételes körülmények között képesek az önkéntes hozzájárulásra, akkor, amikor az ajánlat elfogadásához vagy elutasításához semmilyen következmény nem kapcsolódik.

Jogalapként esetenként hivatkozni lehet a munkáltató jogos érdekére, de csak akkor, ha az adatkezelés törvényes célból feltétlenül szükséges, és megfelel az arányosság és a

szubszidiaritás elvének. Bármilyen megfigyelési eszköz alkalmazása előtt vizsgálni kell az arányosságot, azaz meg kell vizsgálni, hogy valamennyi adat szükséges-e, hogy az adatkezelés előnyt élvez-e a munkavállalók magánélet tiszteletben tartásához fűződő, a munkahelyen is fennálló általános jogaival szemben, és hogy milyen intézkedésekre van szükség annak biztosításához, hogy a magánélet tiszteletben tartásához és a közlés titkosságához fűződő jog megsértése a minimálisan szükséges mértékre korlátozódjon.

6.3 Átláthatóság

A munkavállalók számára érdemi tájékoztatást kell nyújtani az alkalmazott számára a megfigyelésről, annak céljáról és körülményeiről, valamint arról, hogy a munkavállalóknak milyen lehetőségük van az adataik megfigyelési technológiák alóli kivonására. A jogszerű megfigyelésre vonatkozó politikáknak és szabályoknak egyértelműeknek és könnyen elérhetőeknek kell lenniük. A munkacsoport javasolja, hogy vonják be a munkavállalók egy reprezentatív mintáját az ilyen politikák és szabályok kidolgozásába és értékelésébe, mivel a megfigyelés legtöbb formája potenciálisan sértheti a munkavállalók magánéletét.

6.4 Arányosság és adatminimalizálás

A munkahelyi adatkezelésnek a munkáltatót érintő kockázatokkal arányos válasznak kell lennie. Az internet nem megfelelő használata például a honlapok tartalmának elemzése nélkül is felderíthető. Ha a visszaélés (pl. webszűrő alkalmazásával) megelőzhető, a munkáltató nem jogosult általános megfigyelést folytatni.

A magáncélú kommunikáció teljes tilalma például nem praktikus, és a tilalom érvényesítése aránytalan mértékű megfigyelést tehet szükségessé. Sokkal nagyobb súlyt kell helyezni a megelőzésre, mint a felderítésre: a munkáltató érdekét jobban szolgálja az internet nem megfelelő használatának műszaki eszközökkel történő megelőzése, mint az, ha erőforrásait a visszaélés felderítésére kell fordítania.

A folyamatos megfigyelésből származó adatok rögzítését és a munkáltató számára elérhetővé tett információkat a lehető legkisebb mértékűre kell csökkenteni. A munkavállalók számára lehetővé kell tenni, hogy ha ezt a körülmények indokolják, ideiglenes kiiktathassák a tartózkodási hely nyomon követését. A járműkövetési megoldások például kialakíthatók úgy, hogy a tartózkodási helyre vonatkozó adatokat anélkül rögzítsék, hogy azokat a munkáltatónak megjelenítsék.

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

6.5 Felhőalapú szolgáltatások, online alkalmazások és nemzetközi adattovábbítás

Amennyiben a munkavállalóknak személyes adatokat kezelő online alkalmazásokat (pl. online irodai alkalmazásokat) kell használniuk, a munkáltatónak meg kell fontolnia, hogy lehetőséget biztosítson a munkavállalóknak magáncélú terek, például magánjellegű levél- vagy dokumentummappa kijelölésére, amelyhez a munkáltató semmilyen körülmények között nem fér hozzá.

A legtöbb felhőalapú alkalmazás használata a munkavállalók adatainak nemzetközi továbbításával jár. Biztosítani kell, hogy személyes adatok Unión kívüli harmadik országba történő továbbítására csak akkor kerüljön sor, ha a védelem megfelelő szintje biztosított, valamint hogy az adatok Unión/EGT-n kívüli megosztása, valamint azt követően a csoporthoz tartozó más felek általi hozzáférés továbbra is az adott célhoz szükséges legkisebb mértékűre korlátozódjon.

* * *

Készült Brüsszelben, 2017. június 8-án

A munkacsoport részéről
az elnök,
Isabelle FALQUE-PIERROTIN