Tavaszi megújulás - Új adatvédelmi követelmények májustól

Budapest, 2019. május 9.

DR. OSZTOPÁNI KRISZTIÁN
DR. GYÖRGY ANDRÁS

I.

Jogszabályi változások

A GDPR miatt változó jogszabályok

Az Országgyűlés 2019. április 1-jén fogadta el „a GDPR salátatörvény” módosítást, amely 86 törvényt módosított a GDPR-nak való megfelelés érdekében.

- **munkahelyi adatkezelésre vonatkozó szabályok**
- **kamerás megfigyelőrendszer üzemeltetése („általános”, társasház, személyszállítási szolgáltatók)**
- **visszaélés-bejelentő rendszer (whistleblowing) működtetése**

1. Okmánymásolatok készítése

Az Mt. 10. § (3) bekezdése alapján nyilatkozat megtételéhez vagy személyes adat közléséhez kapcsolódóan csak az "*okirat bemutatása követelhető*."

NAIH 2018. szeptember 28-ai állásfoglalása:

- **a személyazonosító okmányok közhitelesek**
- **az okmányokról készített másolat nem rendelkezik olyan bizonyító erővel, hogy hiteles másolata egy hatósági okmánynak**
- **kényelmi szempontok vagy „gyorsabb ügyintézés" szintén nem indokolhatják a másolat készítését**

1. Okmánymásolatok készítése

NAIH javaslata az okmánymásolat készítésének alternatívájaként:

- **Az adatkezelő ügyintézője egy nyilatkozat kitöltését kéri az érintettől arról, hogy mely hatósági okmányát mutatta be.**

- **A „négy szem elve”: egy másik ügyintéző vagy az ügyintéző felettese is megtekinti az érintett által bemutatott okmányt, és ő is megerősíti a személyazonosságot és a rögzített adatok pontosságát.**

Ha jogszabály vagy hatósági rendelkezés írja elő az okmánymásolat készítését, akkor az felülírja az Mt. rendelkezését.

2. Erkölcsi bizonyítványok kérése

Az Mt. új 11. § (3)-(5) bekezdései szabályozzák azt, hogy milyen feltételek teljesülése esetén kérhet erkölcsi bizonyítványt a munkáltató.

1. ***Ha a törvény elrendeli*. Például 18 éven aluli személyek nevelését, felügyeletét, gondozását, gyógykezelését végző munkavállaló.**
2. **Ha a munkavállaló foglalkoztatása a *munkáltató jelentős vagyoni érdeke* sérelmének veszélyével járna.**
3. **Ha a munkavállaló foglalkoztatása a *törvény által védett titok* (így például üzleti titok, védett ismeret) sérelmének veszélyével járna.**

2. Erkölcsi bizonyítványok kérése

4. Ha a munkavállaló foglalkoztatása lőfegyver, lőszer, robbanóanyag, mérgező vagy veszélyes vegyi anyag, nukleáris anyag őrzésével jár együtt.

A 2.-4. pontok esetében munkáltatónak kell igazolnia, hogy az estében mely munkakörök vonatkozásában, miért merül fel az adott körülmény.

A munkáltatónak érdekmérlegelési tesztet kell elkészítenie, illetve előzetes tájékoztatnia kell a munkavállalót.

Kizárólag az okmány bemutatása követelhető meg.

2. Erkölcsi bizonyítványok kérése

Az erkölcsi bizonyítványokkal szembeni kritika:

- **Csak annak igazolására alkalmas, hogy szerepel-e nyilvántartásban, azt azonban nem mutatja meg, hogy van-e vele szemben folyamatban büntetőeljárás.**

- **Olyan bűncselekmények is lehetnek, amelyről az adott személy nem feltétlenül szeretne számot adni, de nem is befolyásolja a munkakör ellátását.**

- **A bizonyítvány vagy másolatának tárolása azért sem szükséges, mivel észszerűen nem képzelhető el olyan eljárás, ahol ezt bizonyítékként fel kellene használni.**

3. Biometrikus beléptető rendszer

Az Mt. 11. § (1) bekezdése alapján biometrikus beléptető rendszer alkalmazásnak feltételei:

1. **Az érintett azonosítása céljából alkalmazható.**
2. **Ha valamely dologhoz, adathoz való jogosulatlan hozzáférés vagy elzárt területre való belépés megakadályozásához szükséges.**
3. **Teljesüljön az Mt. szerinti jogos érdek.**
4. **Annak igazolása, hogy valamely jogellenes magatartás ezen jogos érdek súlyos vagy tömeges, visszafordíthatatlan sérelmének a veszélyével jár.**

3. Biometrikus beléptető rendszer

Az Mt. 11. § (1)-(2) bekezdése alapján jogos érdek:

- **a munkavállaló vagy mások élete, testi épsége vagy egészsége**
- **a legalább „Bizalmas!” minősítési szintű minősített adatok védelme**
- **a lőfegyver, lőszer, robbanóanyag őrzése**
- **a mérgező vagy veszélyes vegyi vagy biológiai anyagok, illetve a nukleáris anyagok őrzése**
- **a Btk. szerint legalább különösen nagy vagyoni érték védelme (50 millió forint feletti vagyon)**

4. Munkahelyi informatikai eszközök

Az Mt. 11/A. § (2) bekezdése főszabályként kimondja: "*a munkavállaló a munkáltató által a munkavégzéshez biztosított információtechnológiai vagy számítástechnikai eszközt, rendszert (a továbbiakban: számítástechnikai eszköz) – eltérő megállapodás hiányában – kizárólag a munkaviszony teljesítése érdekében használhatja.*"

Vagyis a munkáltató dönthet úgy, hogy a munkavállalók használhatják magáncélra az informatikai eszközöket.

Ez azzal a kockázattal jár, hogy az eszközök merevlemezén és a biztonsági mentéseken rajta lehetnek a munkavállaló személyes adatai.

4. Munkahelyi informatikai eszközök

Az Mt. 11/A. § (3) bekezdése rögzíti, hogy "*a munkáltató ellenőrzése során a munkaviszony teljesítéséhez használt számítástechnikai eszközön tárolt a munkaviszonnyal összefüggő adatokba tekinthet be.*"

Az ellenőrzés megkezdését megelőzően a munkavállalónak nyilatkoznia kell arról, hogy a számítástechnikai eszközön tárol-e személyes adatokat.

Ha igen, akkor az adatokat külső meghajtóra kell átmásolni. Ezen külső adathordozót kizárólag indokolt esetben vizsgálhatja meg a munkáltató.

4. Munkahelyi informatikai eszközök

Az Mt. 11/A. § (4) bekezdése értelmében "*a (3) bekezdés szerinti ellenőrzési jogosultság szempontjából munkaviszonnyal összefüggő adatnak minősül a (2) bekezdésben meghatározott korlátozás betartásának ellenőrzéséhez szükséges adat.*"

A munkáltató nem követ el jogellenes adatkezelést, ha az ellenőrzés során személyes adatot tartalmazó fájlt nyit meg (például fénykép fájlt), mivel a fájl elnevezéséről vagy arról, hogy melyik mappában található, nem lehetett eldönteni, hogy az "munkáltatói adatnak" vagy személyes adatnak minősül-e.

4. Munkahelyi informatikai eszközök

Az Mt. 11/A. § (5) bekezdése kimondja, hogy "*a (3) bekezdést alkalmazni kell, ha a felek megállapodása alapján a munkavállaló a munkaviszony teljesítése érdekében saját számítástechnikai eszközt használ.*"

„Bring your own device”: a saját eszköz használatának engedélyezésével a munkáltató a rugalmas, a munkavállalói elvárásokhoz való alkalmazkodását mutatja, és növeli a termelékenységet.

Ugyanakkor jelentős adatbiztonsági kockázatot hordoz magában, éppen ezért pontos szabályozást igényel, hogy milyen feltétel mellett használhatók a saját készülékek.

5. Vásárlók könyve

A kereskedelemről szóló törvény 5. § (4a) bekezdése:

„Más vásárlók által a vásárlók könyvébe bejegyzett személyes adatok megismerése lehetőségének kizárása céljából a vásárlók könyvéből a kereskedő a bejegyzést követően haladéktalanul eltávolítja a (4) bekezdés szerint panaszt vagy javaslatot tartalmazó oldalt, azt elzártan – a folyamatos sorszámozás rendjének megfelelően – megőrzi és a hatóság felszólítására rendelkezésre bocsátja.”

6. Visszaélés-bejelentési rendszerek

Jelentősen módosultak, illetve észszerűbbé váltak a 2013. évi CLXV. törvénynek (Pktv.) a munkáltatói visszaélés-bejelentési rendszerre vonatkozó rendelkezések:

1. **A törvénymódosítás hatályon kívül helyezte a különleges adatok kezelésére vonatkozó tilalmat: a bejelentés kivizsgálásához szükséges különleges és bűnügyi személyes adatokat kezelheti az adatkezelő.**

2. **Külföldi adattovábbítás esetén a címzettnek vállalnia kell, hogy megtartja a Pktv. rendelkezéseit (+ alkalmazni kell GDPR-nak a harmadik országba történő adattovábbításra vonatkozó rendelkezéseit).**

7. Kamerás megfigyelés változásai

A módosítást követően az Szvtv.-ből kikerült:

- a hozzájárulás jogalapja
- az adatkezelés céljára vonatkozó rendelkezés
- az adatkezelés időtartamára vonatkozó rendelkezés
- a felvételek felhasználására vonatkozó rendelkezés
- a felvételek zárolására vonatkozó rendelkezés
- a felvételekhez való hozzáférésre vonatkozó rendelkezés
- az, hogy a vagyonőrzési feladatot ellátó személy adatkezelőnek minősül

7. Kamerás megfigyelés változásai

A módosítás alapján az Szvtv.-ben az alábbi kötelezettségek maradnak meg:

- **elektronikus megfigyelőrendszert kizárólag magánterületen alkalmazható**
- **nem alkalmazható elektronikus megfigyelőrendszer olyan helyen, ahol a megfigyelés az emberi méltóságot sértheti**
- **a felvételek visszanézéséről jegyzőkönyvet kell felvenni**
- **tájékoztatási kötelezettség**

7. Kamerás megfigyelés változásai

A GDPR alapján az alábbi adatvédelmi követelményeket kell alkalmazni a kamerás megfigyelőrendszerre:

1. **Jogos érdek jogalapjának alkalmazása és érdekmérlegelési teszt elkészítése.**

2. **Adatvédelmi hatásvizsgálat abban az esetben, ha „nyilvános hely nagy mértékű megfigyelése” kitétel fennáll.**

3. **Előzetes tájékoztatási kötelezettség.**

7. Kamerás megfigyelés változásai

Az érdekmérlegelés jogalapjának [GDPR 6. cikk (1) bekezdés f) pont] ismérvei:

- **nem szükséges az érintett hozzájárulása**
- **az adatkezelő vagy harmadik fél megfelelő jogos érdekkel rendelkezik**
- **az adatkezelőnek igazolnia kell azt, hogy a jogos érdekei teljesülése érdekében az érintettek érdekét figyelembe vevő garanciális intézkedéseket vezetett be**

7. Kamerás megfigyelés változásai

1. ***A jogos érdek azonosítása***.

- A jogos érdek nem csak vagyonvédelem, készpénz vagy üzleti titok védelme, lehet: balesetek körülményeinek tisztázása, a vásárlók kényelmesebb kiszolgálása.
- Az adatkezelés konkrét legyen: annak meghatározása, milyen események bekövetkezése esetén hasznos a kamera felvételei.
- Valódi, aktuális, tényszerű jogos érdek legyen, amelyre az adatkezelő tevékenységét tekintve észszerűen számolni lehet.

7. Kamerás megfigyelés változásai

2. *Az adatkezelés szükségességének bemutatása*

- Az adatkezelő által meghatározott jogos érdek észszerűen más módszerrel elérhető-e? Van-e az érintett szempontjából kevésbé korlátozó megoldás?
- Milyen érdekeket szolgál a kamerás megfigyelés: a jogsértés megelőzés, bizonyítása.
- Milyen hátrány érné az adatkezelő abban az esetben, ha nem alkalmazhatna kamerás megfigyelőrendszert?

7. Kamerás megfigyelés változásai

3. *Az adatkezelés arányosságának bemutatása*

- az érintett érdeke kisebb vagy nagyobb részben egybeesik az adatkezelő érdekeivel
- az érintett és az adatkezelő kapcsolata
- az adattakarékosság elve megvalósul
- az adatkezelés időtartamának a lehető legrövidebb időre korlátozása
- annak vizsgálata, hogy a kamerák elhelyezése, látószöge, mennyire kelthet megfigyeltség-érzetet az érintettben

7. Kamerás megfigyelés változásai

3. *Az adatkezelés arányosságának bemutatása*

- annak igazolása, hogy a kamerák üzemeltetése nem sérti az emberi méltóságot
- meghatározott személyi kör férhet hozzá a személyes adatokhoz, meghatározott eljárásrendben
- a felvételek felhasználása csak korlátozott esetben lehetséges
- alapvető biztonsági intézkedések

7. Kamerás megfigyelés változásai

Általános tilalmi szabály: nem lehet kamerát elhelyezni olyan helyiségben, amelyben a megfigyelés az emberi méltóságot sértheti (például öltözők).

Továbbá a Hatóság ajánlása kimondja, hogy alkalmazni az olyan helyiségben sem lehet, amely a munkavállalók munkaközi szünetének eltöltése céljából lett kijelölve (például az ebédlő).

Ez alól kivételt jelenthet az az esetkör, ha ebben a helyiségben valamilyen védendő vagyontárgy található, amellyel összefüggésben igazolható a munkáltató jogos érdeke.

7. Kamerás megfigyelés változásai

A GDPR 35. cikk (3) bekezdés c) pontja alapján hatásvizsgálat elvégzése szükséges nyilvános helyek nagymértékű, módszeres megfigyelése esetén.

NAIH honlapján nyilvánosságra hozott adatvédelmi hatásvizsgálatban:

- **be kell mutatni a kamerás megfigyelőrendszer üzemeltetéséhez kapcsolódó felelősségi viszonyokat**
- **be kell mutatni az adatkezelés teljes folyamatát**
- **az érintetti kérelmek teljesítésének bemutatása**

7. Kamerás megfigyelés változásai

A felvételekhez való jogosulatlan hozzáféréssel vagy a felvételek elvesztésével összefüggésben be kell mutatni:

- **következmények az érintettre nézve (például: emberi méltóság sérelme, jóhírnév sérelme, az eljárás elmaradása)**
- **veszélyforrások (emberi tényező, külső tényezők)**
- **milyen kockázatkezelő intézkedéseket alkalmaz (szabályzat, naplózás, biztonsági mentés, fizikai hozzáférésvédelem)**
- **súlyosság értékelése (egyszerű bosszúság, nyilvánosság előtti beazonosíthatóság, a bizonyítás megnehezülése)**
- **kockázat valószínűségének értékelése**

7. Kamerás megfigyelés változásai

A kamerás megfigyelőrendszerekkel együtt járó adatkezelés esetében a tájékoztatási kötelezettség elemei [Szvtv. 28. § (2) bekezdés c) és d) pontja]:

1. **figyelemfelhívó jelzést kell elhelyezni arról a tényről, hogy az adott területen kamerás megfigyelőrendszert alkalmaznak (például piktogram)**

2. **adatkezelési tájékoztató készítése és kihelyezése**

7. Kamerás megfigyelés változásai

Az adatkezelési tájékoztatóban ki kell térni arra, hogy

- az adatkezelő kiléte (adatvédelmi tisztviselő)
- az adatkezelés jogalapja, és az adatkezelő jogos érdeke
- a felvételek tárolásának időtartam
- a felvétel tárolásának helye
- az Infotv. szerinti érintettek jogai, jogérvényesítési lehetőségek

II.

Szemelvények a NAIH gyakorlatából

NAIH gyakorlata

1. *Az érdekmérlegelési teszttel kapcsolatos megállapítások*

Amennyiben több adatkezelést végez az adatkezelő, akkor adatkezelésenként külön-külön kell elvégezni az érdekmérlegelési tesztet.

Habár a NAIH adatkezelési célokról ír a határozatában, azonban sok esetben valamely adatkezelésnek több célja lehet, ilyenkor elegendő egy érdekmérlegelési teszt (például követelés érvényesítése, egyeztetés, fizetési könnyítési lehetőségek felajánlása).

NAIH gyakorlata

2. Az érintett azonosítása

GDPR 12. cikk (5) bekezdés d) pontja értelmében: ha az adatkezelőnek megalapozott kétségei vannak a kérelmet benyújtó természetes személy kilétével kapcsolatban, akkor az érintett személyazonosságának megerősítését kérheti.

Csak arra az adatra terjedjen ki, ami rendelkezésre áll (például, hogy a születési dátum nem áll rendelkezésre, akkor azt nem kérheti be azonosítás céljából).

NAIH gyakorlata

3. *Az adatkezelés korlátozása az adatok pontatlansága esetén*

GDPR 18. cikk (1) bekezdés a) pontja alapján, ha az értintett vitatja a személyes adatok pontosságát, akkor az adatok pontossága ellenőrzésének idejére zárolni kell a személyes adatokat.

Ha nem biztos abban az adatkezelő, hogy az érintetthez tartozik a személyes adat, akkor korlátozza az adatkezelést arra az időtartamra, amíg ezt tisztázza.

NAIH gyakorlata

4. Az adatkezelés korlátozása jogi igény érvényesítése esetén

A GDPR 18. cikk (1) bekezdés c) pontja alapján a személyes adatokat zárolni kell, ha az adatkezelőnek már nincs szüksége a személyes adatokra, de az érintett igényli azokat jogi igények előterjesztéséhez.

Az adatkezelő nem mérlegelheti a korlátozási kérelem teljesítése során, hogy a személyes adat, amely tekintetében az érintett az adatkezelés korlátozását kérte, alkalmas, illetve szükséges-e jogi igény érvényesítésére.

NAIH gyakorlata

5. Érintetti joggyakorlás elősegítése

GDPR 12. cikk (2) bekezdés: az adatkezelő elősegíti az érintetti jogok gyakorlását.

Az adatkezelő adjon pontos felvilágosítást arról, hogy milyen eljárásrendben tudja gyakorolni a jogait (például elegendő a bemutatás, és nem szükséges a becsatolás).

Amennyiben az adatkezelő lehetővé teszi azt, hogy ha az érintett postai úton forduljon az adatkezelőhöz, akkor erre térjen ki a tájékoztatás során.

NAIH gyakorlata

6. Adatvédelmi incidensekkel kapcsolatos megállapítások

Az adatvédelmi incidenst akkor is be kell jelenteni, még ha a Hatóság ellenőrzést is indít.

Az, hogy az adatkezelő értékelése szerint nem aktuális személyes adatra vonatkozik az incidens (például régebbi tesztadatbázisra), nem jelenti azt, hogy ezen adatokat ne kellene személyes adatnak tekinteni.

NAIH gyakorlata

6. Adatvédelmi incidensekkel kapcsolatos megállapítások

A GDPR 34. cikk (1) bekezdése alapján, ha adatvédelmi incidens valószínűsíthetően magas kockázattal jár, akkor az adatkezelőnek tájékoztatnia kell az érintettet az adatvédelmi incidensről.

Magas kockázatúnak tekinthető a természetes személyazonosító adatok nyilvánosságra kerülése, mivel ezek birtokában személyazonossággal való visszaélés követhető el (pl. szerződéskötés).

S B G K

EST. 1969

Dr. Osztopáni Krisztián - krisztian.osztopani@sbgk.hu

Dr. György András - andras.gyorgy@sbgk.hu