

ADATVÉDELEM A KÖNYVELŐI GYAKORLATBAN III. – ADATVÉDELMI INCIDENSEK FELISMERÉSE, KEZELÉSE ÉS BEJELENTÉSE

Tisztelt Kollégák!

Előző hírleveleinkben az adatvédelem alapjait, majd az adatfeldolgozói szerződést tekintettük át: tisztáztuk, mikor jár el a könyvelő adatkezelőként, mikor adatfeldolgozóként, és milyen szerződéses garanciák szükségesek ehhez. Adatvédelmi sorozatunk következő részében azt vizsgáljuk meg, mi a teendő akkor, ha a megelőző intézkedések ellenére mégis baj történik: hogyan kell felismerni, kezelni, és – szükség esetén – bejelenteni az adatvédelmi incidenseket.

I. MI MINŐSÜL ADATVÉDELMI INCIDENSEK?

Adatvédelmi incidensnek minősül a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi.¹ A fogalom tehát három, egymástól elkülöníthető esetkört ölel fel:

1. a bizalmas jelleg sérülését (jogosulatlan/véletlen hozzáférés vagy közlés),
2. az integritás, azaz a sértetlenség sérülését (jogosulatlan/véletlen megváltoztatás), valamint
3. a rendelkezésre állás sérülését (jogosulatlan/véletlen adatvesztés vagy időleges hozzáférhetetlenné válás).

A könyvelői gyakorlatban tipikusan az alábbi adatvédelmi incidensek fordulhatnak elő:

- **Elveszett vagy ellopott adathordozó:** bérszámfejtési vagy ügyféladatokat tartalmazó, titkosítatlan laptop, pendrive, illetve irat elvesztése, ellopása.
- **Téves címzés:** személyes adatot tartalmazó e-mail vagy dokumentum rossz címzettnek történő elküldése.
- **Jogosulatlan hozzáférés:** a könyvelőprogramhoz, illetve az elektronikus azonosítási / tárhely (például Ügyfélkapu+, DÁP vagy Cégek) hozzáférésekhez való illetéktelen belépés, vagy ha egy illetéktelen személy megszerez, lemásol iratokat.
- **Zsarolóvírus/hacker támadás:** olyan informatikai támadás, amely az adatokhoz való hozzáférést vagy azok sértetlenségét veszélyezteti.

¹ GDPR. 4. cikk 12. pont

- **Gondatlan iratmegsemmisítés:** papíralapú személyi anyagok, bérjegyzékek szabályszerű iratmegsemmisítés helyett történő, nem megfelelő – például hulladékba – kidobása. (A NAIH gyakorlatában is előfordult már, hogy kifejezetten emiatt szabtak ki adatvédelmi bírságot egy könyvelőirodával szemben.)

Fontos hangsúlyozni, hogy nem minden informatikai üzemzavar vagy adminisztratív hiba minősül adatvédelmi incidensnek: kizárólag akkor beszélhetünk ilyenről, ha az esemény ténylegesen személyes adatot érint.

II. AZ INCIDENSKEZELÉS BELSŐ LÉPÉSEI

Az incidens észlelését követően haladéktalanul, előre meghatározott lépések szerint célszerű eljárni:

1. **Felderítés és rögzítés:** mikor és hogyan észlelték az eseményt, milyen rendszereket és adatköröket érint.
2. **Kárenyhítés:** a további károk megelőzését szolgáló azonnali technikai intézkedések – például jelszócsere, hozzáférés visszavonása, az érintett rendszer leválasztása.
3. **Kockázatértékelés:** hány érintettet és milyen adatkört érint az esemény, és milyen súlyú következményekkel (például azonosításalapú visszaélés, pénzügyi kár, hátrányos megkülönböztetés) járhat.

III. AZ ADATKEZELŐ ÉRTESÍTÉSE

Amennyiben az incidens a könyvelő *adatfeldolgozó tevékenysége* során – például a megbízó munkavállalóinak bérszámfejtési adatai körében – következik be, a könyvelő indokolatlan késedelem nélkül köteles arról tájékoztatni a megbízót mint adatkezelőt, és segíteni őt a hatósági bejelentés teljesítésében.²

Ennek kiemelt jelentősége van: az alább ismertetett 72 órás bejelentési határidő ugyanis az adatkezelőnél akkor kezd el telni, amikor ő maga tudomást szerez az incidensről. Ha a könyvelő késlekedik a jelzéssel, a megbízó gyakorlatilag esélytelen helyzetbe kerülhet a határidő megtartása szempontjából. Ezért javasolt, hogy az adatfeldolgozó szerződés – amelyről előző hírlevelünkben írtunk – konkrét, rövid határidőt (például „legkésőbb 24 órán belül”) írjon elő a könyvelő jelzési kötelezettségére.

Amennyiben a könyvelő a saját, önálló *adatkezelői körében* – például saját munkavállalói vagy ügyfél-kapcsolattartói adatai tekintetében – észlel incidenst, úgy már közvetlenül őt terheli a hatóság felé történő bejelentési kötelezettség.

IV. AZ INCIDENS BEJELENTÉSE A NAIH-NAK

Az adatkezelő – a fentiek szerint tehát jellemzően a megbízó, saját adatkezelői körben pedig maga a könyvelő is – az incidenst **indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb a tudásszerzéstől számított 72 órán belül** köteles bejelenteni a Nemzeti Adatvédelmi és Információszabadság Hatóságnak (NAIH). Kivétel ez alól, ha az incidens valószínűsíthetően

² GDPR. 33. cikk (2) bek.

nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Ha a bejelentés nem történik meg 72 órán belül, akkor indokolást kell csatolni a késedelem okáról.³

A bejelentésnek tartalmaznia kell:

- az incidens jellegét, ezen belül az érintettek kategóriáit és hozzávetőleges számát, valamint az érintett adatok kategóriáit és hozzávetőleges számát;
- az adatvédelmi tisztviselő vagy más kapcsolattartó nevét és elérhetőségét;
- az incidensből eredő, valószínűsíthető következményeket;
- a megtett vagy tervezett intézkedéseket, ideértve a károk enyhítését célzó lépéseket is;
- illetve ezen kívül bármilyen további fontos körülményt.⁴

Amennyiben valamennyi adat egyidejűleg nem áll rendelkezésre, a bejelentés szakaszosan is megtehető. A bejelentést elsődlegesen a NAIH Incidensbejelentő Rendszeren (<https://dbn-online.naih.hu/public/login>) keresztül kell megtenni. Az elektronikus ügyintézésre kötelezettek alternatív megoldásként e-papír szolgáltatáson keresztül is megtehetik a bejelentést. Az elektronikus ügyintézésre nem kötelezettek (például természetes személyek) az előzőeken túl postai úton vagy személyesen is benyújthatják bejelentésüket a hatóság által rendszeresített nyomtatvány kitöltésével.⁵

Fontos, hogy a kockázatmentesség megállapítása, vagyis a bejelentés mellőzésének indoka az adatkezelő – a fentiek szerint tehát jellemzően a megbízó saját adatkezelői körben pedig a könyvelő – felelőssége, így őt terheli a bizonyítás: ezt a döntést és annak indokait az elszámoltathatóság elve alapján akkor is dokumentálni kell, ha végül nem történik bejelentés.

V. AZ ÉRINTETTEK TÁJÉKOZTATÁSA

A NAIH felé történő bejelentésen túl, ha az incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az adatkezelő az érintetteket is köteles indokolatlan késedelem nélkül, világosan és közérthető formában tájékoztatni.⁶

Mikor beszélünk magas kockázatról? A GDPR nem határozza meg tételesen a magas kockázat fogalmát: azt minden esetben egyedi kockázatértékeléssel kell megállapítani.⁷ A könyvelői gyakorlatban az alábbi szempontok végiggondolása segít az értékelésben:

- Az érintett adatok jellege: különleges adat (például egészségi állapotra, szakszervezeti tagságra utaló adat), illetve olyan adatkör, amelyből közvetlenül pénzügyi veszteség vagy személyazonossággal való visszaélés következhet – tipikusan bérjegyzék, bank-számlaszám, adóazonosító jel, TAJ-szám.
- Lehetséges következmények: hátrányos megkülönböztetés, személyazonosság-lopás, pénzügyi veszteség, jó hírnév sérelme, a szakmai titoktartás alá tartozó adatok bizalmas jellegének sérülése, az álnevesítés jogosulatlan feloldása, illetve bármely egyéb jelentős gazdasági vagy szociális hátrány.
- Az adatok mennyisége és az érintettek száma: nagy adatmennyiség, illetve nagyszámú érintett önmagában is növeli a kockázatot.

³ GDPR 33. cikk (1) bek.

⁴ GDPR 33. cikk (3) bek.

⁵ <https://www.naih.hu/online-ugyinditas/386-az-adatkezo-adatvedelmi-incidens-bejelentese-a-felugyeleti-hatosagnak-gdpr-33-cikk-vagy-infotv-25-j-alapjan>

⁶ GDPR. 34. cikk (1) bek.

⁷ GDPR Preambulum (75) bek.

- Az érintettek rendelkezési lehetősége: elveszítik-e a kontrollt a saját adataik felett, illetve akadályozza-e az incidens a jogaik gyakorlását.
- Az érintettek kiszolgáltatottsága: például gyermekek adatainak érintettsége.
- Az incidens visszafordíthatósága: helyreállítható-e az adat, ismert-e a jogosulatlan hozzáférő személye, illetve titkosítás vagy más intézkedés kizárja-e az adatok érdemi felhasználását.

A gyakorlati tapasztalat szerint a bérszámfejtési és munkaügyi adatokat érintő incidensek jellemzően a magas kockázatú kategóriába tartoznak, mivel jövedelmi, társadalombiztosítási és pénzforgalmi adatok együttes kikerülésével járnak. A kockázatértékelés eredményét – akkor is, ha annak végkövetkeztetése szerint tájékoztatásra nincs szükség – írásban indokolt rögzíteni, mivel egy hatósági eljárásban ez igazolja a döntés megalapozottságát.

A tájékoztatási kötelezettség alól a GDPR három esetben ad felmentést:

- ha az adatkezelő az incidenst megelőzően olyan megfelelő technikai és szervezési intézkedéseket – például titkosítást – alkalmazott, amely az adatokat az azokhoz való jogosulatlan hozzáféréssel szemben értelmezhetetlenné teszi;
- ha az adatkezelő az incidenst követően olyan további intézkedéseket tett, amelyek biztosítják, hogy a magas kockázat a továbbiakban valószínűsíthetően már nem valósul meg;
- ha a tájékoztatás aránytalan erőfeszítéssel járna – ilyenkor nyilvánosan közzétett közleménnyel vagy hasonló hatékony intézkedéssel is teljesíthető a tájékoztatás.⁸

A könyvelő szerepe: Adatfeldolgozói minőségében a könyvelő az érintettek közvetlen tájékoztatására nem jogosult és nem is köteles: ez az adatkezelő, azaz a megbízó feladata. A könyvelőnek azonban közre kell működnie a tájékoztatás teljesítésében, így a kockázatértékeléshez és a tájékoztatás tartalmának összeállításához szükséges információk (érintett adatkörök, érintettek létszáma, incidens időpontja és lefolyása) rendelkezésre bocsátásában.

VI. NYILVÁNTARTÁS, DOKUMENTÁCIÓ, FELELŐSSÉG

Az adatkezelő – így adott esetben a könyvelőiroda a saját adatkezelői körében is – valamilyen adatvédelmi incidenst köteles dokumentálni, függetlenül attól, hogy az a NAIH felé bejelentésre került-e. A nyilvántartásnak tartalmaznia kell az incidenshez kapcsolódó tényeket, annak hatásait és a megtett intézkedéseket. Ez a dokumentáció teszi lehetővé a NAIH számára a jogszabályi megfelelés utólagos ellenőrzését, és egyúttal ez az egyetlen módja annak, hogy az adatkezelő utólag igazolni tudja: a bejelentés mellőzéséről megalapozott kockázatértékelés alapján döntött.⁹

Célszerű ezért már előre, egy esetleges incidens bekövetkezése előtt kialakítani egy *egyszerű belső eljárásrendet*: ki a felelős az észlelt esemény rögzítéséért, kit kell haladéktalanul értesíteni – az irodavezetőt, a megbízót mint adatkezelőt, szükség esetén a jogi képviselőt –, és milyen sablon alapján történik a dokumentálás, illetve szükség esetén a NAIH-bejelentés.

⁸ GDPR 34. cikk (3) bek.

⁹ GDPR 33. cikk (5) bek.

A bejelentési vagy tájékoztatási kötelezettség elmulasztása önálló *jogsértésnek minősül*, amelyért a GDPR szerint kiszabható bírság felső határa 10 millió euró, illetve a vállalkozás éves forgalmának 2%-a közül a magasabb összeg.¹⁰ A hazai gyakorlatban a NAIH a kis- és középvállalkozásokkal szemben jellemzően ennél lényegesen alacsonyabb bírságot szab ki, ugyanakkor egy incidens nyilvánosságra kerülése – a bírságtól függetlenül is – **jelentős bizalomvesztéssel járhat** egy könyvelőiroda számára, amelynek működése az ügyfelek bizalmán alapul.

¹⁰ GDPR 83. cikk (4) bek.

A fenti tájékoztatás nem minősül jogi tanácsadásnak. A csőd-, a kényszertörlési és a végelszámolási eljárás egyaránt összetett, számos határidővel terhelt, és a hitelezői pozíció szempontjából jelentős következményekkel járó eljárás, ezért a konkrét lépések megtétele előtt minden esetben javasoljuk jogi szakember bevonását.

Készítette:

Szabó Kocsis Ügyvédi Iroda



A MINKE jogi partnere