Mi az az adatvédelmi incidens?

"Ha már megtörtént a baj, legalább ne tetézzük!"

szerző: Dr. Albert Ágota, a MÁOK adatvédelmi tisztviselője

Az „adatvédelmi incidens" **a GDPR meghatározása alapján 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.**

Azaz teljesen mindegy, hogy került hozzánk a személyes adat, kezeljük, tároljuk vagy más módon kezeljük és az is lényegtelen, hogy véletlenül történt-e a galiba vagy valaki szándékosan hozta ránk a bajt,

- ✓ amennyiben **az adat megsemmisül** (például egy vírus tönkreteszi a merevlemezünket vagy csőtörés amortizálta le örökre a számítógépünket és a hagyományos irattárunkat is)
- ✓ **elveszítjük az adatot** (elhagyjuk a laptopunkat vagy ellopják a táskánkat az ügyfélnyilvántartásunkat tartalmazó noteszünkkel együtt)
- ✓ **valaki megváltoztatja az adatot** (például adminisztrátorunk kis tudás nagy tudatlanság birtokában, cserébe hihetetlen elszántsággal és lelkesedéssel felülírja a jó adatainkat rosszakkal, jól összekutyulva mindent, amihez csak hozzáfér)
- ✓ **valaki a mi adatainkat jogosulatlanul közli** (például valaki önmagát oknyomozó újságírónak kiáltva ütős bulvárhírnek összeeszkábálva közzéteszi az interneten, hogy melyik celeb felejti el időben beoltatni az ölebét, amelyik ráadásul még fogköves is), vagy netalán
- ✓ **valaki jogosulatlanul fért hozzá az adatainkhoz** (az adminisztrátorunk megtalálta a billentyűzetünk hátoldalára ragasztott jelszavunkat és a mi távollétünkben végignézte, hogy a sógora utcájában kinek milyen drága fajmacskája meg egyéb jószága van),

az adatvédelmi incidens megtörtént, mi pedig gondolkodhatunk, **hogyan is mászszunk ki a slamasztikából.**

A GDPR szempontjából azért **kiemelt feladat az adatvédelmi incidens megelőzése**, mert **az adatvédelmi incidens megfelelő és kellő idejű intézkedés hiányában fizikai, vagyoni vagy nem vagyoni károkat okozhat a természetes személyeknek**, többek között

- ✓ a személyes adataik feletti rendelkezés elvesztését vagy a jogaik korlátozását,
- ✓ hátrányos megkülönböztetést,
- ✓ személyazonosság-lopást vagy a személyazonosságukkal való visszaélést,
- ✓ pénzügyi veszteséget,
- ✓ az álnevesítés engedély nélküli feloldását,

- ✓ a jó hírnév sérelmét,
- ✓ szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülését, illetve
- ✓ egyéb jelentős gazdasági vagy szociális hátrányt.

Feltétlen ki kell emelni, **nem kell, hogy az adatok** (vagy akár egyetlen adat is) **jogellenesen napvilágra kerüljenek, vagy az érintettnek bármilyen kára származzon az incidensből, az incidens már abban a pillanatban megvalósult, amikor az adat véletlenül vagy jogellenesen megsemmisült, elveszett, megváltozott vagy ahhoz bárki jogosulatlanul hozzáfért**. És az is nagyon fontos, hogy az adatvédelmi incidens a biztonság sérülésén keresztül van meghatározva, azaz a GDPR elvárja, hogy a biztonság ne csak egy jogszabályi fordulat legyen, hanem a gyakorlatban is ügyködjünk az általunk kezelt adatok biztonságának optimális szintjének elérése érdekében.

Nem kell feltétlenül egetverő dolgokra gondolnunk, amikor a biztonsági intézkedésekre gondolnunk. Ha be akarnak törni hozzánk, akkor úgyis betörnek, de ha riasztó rendszerünk van, akkor kisebb az esélye, hogy a tolvaj sokat időzve és matatva, fülsiketítő szirénaüvöltés mellett a belső bezárt helyiségben lévő bezárt szekrényünkből emelne el valamit. A csőtörést sem tudjuk megelőzni, de azért arra ügyelhetünk, hogy ne a felettünk tanyázó bérlő vizesblokkja alatt tároljuk az informatikai eszközeinket, illetve rendszeres biztonsági mentéssel, fontosabb irataink digitalizálásával és archiválásával már előre enyhíthetünk a káron, aztán ha úszik az irodánk, legalább az adataink egy részét képesek leszünk visszaállítani.

Sőt, a GDPR azt szeretné, hogy már **jó előre tegyünk meg mindent annak érdekében, hogy igenis gondos családapaként tudjuk vigyázni a mások ránk bízott adataira**. Legyen olyan erős jelszavunk, amely nincs kiragasztva a monitorunkra, ne csak telepítsünk vírusirtót, hanem kellő gyakorisággal frissítsük is azt, ne használjunk olyan kalózszoftvereket, amelyek a jelenleg ismert világunk túlsó felére küldözgetik tudtunk nélkül az adatainkat. És valljuk be, az is elvárható magatartás, hogy az irataink ne hagyjuk szanaszét, hanem zárható szekrényben őrizzük, a laptopunkat pedig ne felejtsük a kocsink hátsó ülésén addig, amíg beugrunk a sarki üzletbe vacsorának valóért. **Nem Fort Knoxot kell újraépítenünk az adataink köré, hanem leginkább a józan eszünket kell használnunk az adatkezelésünkkel együtt járó kockázat minimalizálása érdekében.**

Azonban bárhogy is próbáljuk megelőzni, még a legkörültekintőbbeket is utolérheti a végzet adatvédelmi incidens formájában, amit ráadásul 2018. május 25. óta **önfeljelentés formájában a Hatósággal is tudatnunk kell 72 órán belül.** A Hatóság pedig még segít is nekünk – 26 oldalas nyomtatványt bocsát a rendelkezésünkre, amit aztán kitöltve beküldhetünk. **Ha megtörtént a baj, nem szabad sunnyogni, szőnyeg alá söpörni a problémát**, azt pedig mindenképpen próbáljuk elkerülni, hogy a 71. órában álljunk neki a bejelentés hatóságilag kiadott kérdőívét először elolvasni.

Milyen forgatókönyvre számíthatunk egy adatvédelmi incidens esetén?

Tegyük fel, hogy észleljük, belecsöppentünk egy adatvédelmi incidens közepébe. Ebben az esetben, **akinek először feltűnt, hogy baj van, annak kutya kötelessége ezt haladéktalanul jelenti a szervezet vezetőjének**, a Kamara esetében pedig nem csak a főnöknek kell szólni, hanem a főtitkáron keresztül az adatvédelmi tisztviselőnek is.

Előre alakítsunk ki helyi protokollt arra (ez a hatóság elvárása is, és nemcsak a kialakítás, hanem a rendszer tesztelése is), hogy ez a jelentés milyen formában történjen, azaz pontosan adjuk meg, miről kell beszámolni az első döbbenet lecsengése után. A legjobb, ha kész blankettánk van a bejelentéshez, így semmi sem marad ki. A legfontosabb információk, amelyeket tovább kell adni:

- ✓ az incidens észlelőjének neve és elérési adatai (telefonszám, e-mail cím)
- ✓ nagyobb szervezet esetén az sem árt, ha tudjuk, melyik szervezeti egységhez tartozik a bejelentő, illetve melyik szervezeti egységnél történt a baj,
- ✓ le kell még írni, mi is történt valójában (incidens tárgya és rövid leírás), és az is lényeges, hogy
- ✓ az incidens informatikai rendszert érint-e.

A blankettán legyen hely még olyan további fontos információknak is, amelyek segítenek az incidens kivizsgálásában és fontosak a kárelhárítás szempontjából. **Amennyiben az adatvédelmi incidens érinti az informatikai rendszert, abban az esetben az informatikai rendszerért felelős személynek is szólni kell**. Sőt, **ha a szervezet adatfeldolgozóként kezel adatokat más nevében, úgy az adatfeldolgozót is haladéktalanul értesíteni kell.**

Az értesítés alapján a szervezet vezetőjének a felelőssége, hogy a bejelentésben foglaltakat megvizsgálja, illetve – amennyiben az szükséges – további tájékoztatást kérjen a bejelentőtől. A vizsgálat során nem lehet lazsálni, az óra ketyeg, az úgy döntünk, hogy nem döntünk taktika alkalmazása pedig ebben az esetben akár súlyos bírságot is eredményezhet.

Mire kell kiterjednie az újonnan bekért tájékoztatásnak? Mindenre, ami az ügy szempontjából fontos és erre is legyen blankettánk, hogy még véletlenül se maradjon ki semmi fontos.

Legyen benne

- ✓ az incidens bekövetkezésének időpontja és helye,
- ✓ az incidens leírása, körülményei és hatása,
- ✓ az incidens során kompromittálódott adatok köre és számossága,
- ✓ a kompromittálódott adatokkal érintett személyek köre,
- ✓ az incidens elhárítása érdekében tett intézkedések leírása,
- ✓ a kár megelőzése, elhárítása, csökkentése érdekében tett intézkedések leírása.

Természetesen **a szervezet vezetőjének nem kell egyedül vizsgálódnia, a feladattal megbízhat olyan személyt, aki ért az ilyen helyzetekhez**, a Kamara azon szervezetinek esetében pedig, akik korábban szerződtek a GDPR dokumentumok elkészítésére, az adatvédelmi tisztviselő bevonása nélkülözhetetlen.

A bejelentés, vizsgálat és részletes tájékoztató alapján a legfontosabb az érintettek védelme – azaz mindent meg kell tennünk annak érdekében, hogy a kárelhárítás, kárenyhítés és a szokásos üzletmenet visszaállítása a lehető leghamarabb megtörténjen. A konkrét intézkedésekről a szervezet vezetője dönt a vizsgálatba bevont személyek javaslatai alapján.

Az adatvédelmi Hatóságnak késedelem nélkül – ha lehetséges, legkésőbb 72 órával az adatvédelmi incidens tudomására jutásától – **be kell jelentenünk az incidenst kivéve akkor, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve.**

Végre egy jó hír – **a GDPR rendelkezései alapján nem kell az összes adatvédelmi incidens bejelenti, a mentességet élvező esetek számának aránya pedig rajtunk is múlik**.

Például trehányak voltunk és nem találjuk a hordozható memóriánkat. Ugyan kötöttünk is jó nagy színes masnit a kétcentis kütyüre, de így sincs meg és már a reményt is feladtuk, hogy valaha is meglegyen, viszont tudjuk, sok-sok személyes adat van rajta és sajnos nem csak a sajátunk. Ez adatvédelmi incidens, elviekben be kellene jelentenünk a hatóságnak. Azonban ha az adatok anonimizálva (álnevesítve) vannak rajta, tehát a valódi érintettekkel az adatok nem kapcsolhatók össze (az álnevek és valódi nevek közös listája egy szekrényben biztos helyen el vannak zárva), akkor munkánk ugyan lesz az adataink helyreállításával, de legalább a hatósághoz nem kell bejelentenünk a gondatlanságunkat.

Akkor sem bejelentendő az adatvédelmi incidens, ha például csőtörés, gázrobbanás, tűz, stb. miatt helyreállíthatatlanul tönkrement a számítógépünk merevlemeze, viszont van olyan biztonsági mentésünk, amelyből az egész rendszerünket újra, maradéktalan adattartalommal fel tudjuk állítani. Azonban ebben az esetben sem szabad hátradőlnünk, mivel az, hogy számunkra helyreállíthatatlanok az adatok még nem azt jelenti, hogy mások számára is az – a sérült merevlemezt nem adhatjuk el, nem dobhatjuk ki csak úgy lazán a kukába, mert nálunk okosabbak, informatikailag felkészültebbek még elővarázsolhatnak adatokat belőle és máris elmondhatjuk, saját magunknak köszönhetjük az újabb adatvédelmi incidenst. **Használt, megunt, vagy saját szempontunkból bármilyen okból lomnak minősített adathordozót tartalmazó kütyüjeinket (PC, laptop, okos telefon, okos óra, tablet, stb.) ne adjuk ki a kezünkből úgy, hogy azokon bármilyen szempontból helyreállítható adatok vannak**, és szervizbe se adjuk be javíttatni egyetlen eszközünket se úgy, hogy azon személyes adatok vannak.

Védekezhetünk még adataink feltörhetetlen kódolásával is, ehhez azonban kérjük hozzáértő szakember segítségét, mert ami a mi számunkra feltörhetetlen, az más számára még nem biztos, hogy az.

Amennyiben a hatósághoz be kell jelentenünk az incidenst, nincs más út, mint az előre – **időben veselkedjünk neki a nyomtatvány kitöltésének**. Ehhez a hatóság többféle verziót is ajánl (https://naih.hu/adatvedelmi-incidensbejelent--rendszer.html). Vigyázzunk, mert egy-két kérdés erősen alkalmas arra, hogy a rájuk adott válaszunkkal még mélyebbre ássuk a gödröt magunk alatt, ezért jól fontoljuk meg minden egyes szavunkat és az sem árt, ha szakember segítségét kérjük a kitöltésez.

A GDPR alapján minimum az alábbi információkat kell közölnünk a Hatósággal:

- ✓ az adatvédelmi incidens jellege, beleértve – ha lehetséges – az érintettek kategóriái és hozzávetőleges száma, valamint az incidenssel érintett adatok kategóriái és hozzávetőleges száma,
- ✓ a további tájékoztatást nyújtó kapcsolattartó neve és elérhetősége,
- ✓ az adatvédelmi incidensből eredő valószínűsíthető következmények.
- ✓ a szervezet által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedések beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

Amennyiben nem lehetséges az információkat egyidejűleg közölni, akkor azokat további indokolatlan késedelem nélkül később részletekben is közölhetjük.

Azonban nemcsak a Hatóságot kell tájékoztatnunk, hanem az érintetteket is, ráadásul indokolatlan késedelem nélkül, valamint világosa és közérthető formában töredelmesen be kell vallanunk nekik, mi a helyzet. **A tájékoztatónkban feltétlen ki kell térnünk az alábbiakra:**

- ✓ a további tájékoztatást nyújtó kapcsolattartó neve és elérhetősége,
- ✓ az adatvédelmi incidensből eredő valószínűsíthető következmények,
- ✓ az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseink, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseinket.

Azonban **nem minden esetben kell tájékoztatnunk az érintette(ke)t**, így például akkor nem, ha

- ✓ titkosítottunk vagy anonimizáltunk (azaz megfelelő technikai és szervezési védelmi intézkedéseket hajtottunk végre és ezáltal jogosulatlanok számára az adatok értelmezhetetlenné váltak)
- ✓ az adatvédelmi incidenst követően olyan további intézkedéseket tettünk, amelyek biztosítják, hogy az érintett jogaira és szabadságaira jelentett magas kockázat a továbbiakban valószínűsíthetően nem valósul meg (például a kiszivárgott, de még jogosulatlan személy által fel nem használt jelszavunkat megváltoztattuk),

- ✓ a tájékoztatás aránytalan erőfeszítést tenne szükségessé. Ebben az esetben az érintetteket nyilvánosan közzétett információk útján, vagy egyéb hasonló módon tájékoztathatjuk.

Az adatvédelmi incidensekről nyilvántartást kell vezetnünk.

A nyilvántartás célja, hogy az incidensekkel kapcsolatos intézkedések ellenőrizhetők legyenek, illetve az érintett tájékoztatása. A Hatóság szerint nem magyarázhatjuk az incidens nyilvántartásba bejegyzésének elmaradását azzal, hogy az érintett tájékoztatása megtörtént, mert ez egyrészt sérti az adatvédelemre vonatkozó törvényt, másrészt megnehezíti, hogy a Hatóság ellenőrizze az adatvédelmi incidenssel kapcsolatos intézkedéseinket.

A nyilvántartásnak tartalmaznia kell az alábbiakat:

- ✓ az érintett személyes adatok köre,
- ✓ az adatvédelmi incidenssel érintettek köre és száma,
- ✓ az adatvédelmi incidens időpontja,
- ✓ az adatvédelmi incidens körülményei, hatásai,
- ✓ az adatvédelmi incidens által bekövetkezendő kár elhárítására megtett intézkedések,
- ✓ az adatkezelést előíró jogszabályban meghatározott egyéb adatok.

A nyilvántartásban szereplő adatvédelmi incidensekre vonatkozó adatok megőrzési ideje:

- ✓ személyes adatokat érintő incidens esetében 5 év,
- ✓ különleges adatokat érintő incidens esetében 20 év.

A nyilvántartásban adatvédelmi incidensben érintett személy személyes adata nem szerepelhet.

Megjegyzés: az említett blanketták a kamarai tagoknak rendelkezésére álló adatvédelmi szabályzat mellékleteiben megtalálhatóak.