Adatvédelmi incidens bekövetkezése esetén követendő eljárásrend

A **Tüke Busz Közösségi Közlekedési Zártkörűen Működő Részvénytársaság** (a továbbiakban: „**adatkezelő**" vagy **„Társaság"**) 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 szóló az Európai Parlament és a Tanács (EU) 2016/679 Rendeletében (a továbbiakban: „**Rendelet**" vagy „**GDPR**"), valamint az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvényben (a továbbiakban: „**Infotv.**") foglaltaknak való megfelelés, az adatvédelem és adatbiztonság rendjének szabályozása végett a Rendelet 5. cikk (2) bekezdésében foglalt elszámoltathatóság elvére és 32. cikkére is tekintettel, adatvédelmi incidens hatékony kezelésének elősegítése érdekében az alábbi eljárásrendet alkotja.

Jelen eljárásrend az elszámoltathatóság elvével összhangban útmutatásul szolgál annak érdekében, hogy a Társaság adatkezelési tevékenysége során bekövetkező adatvédelmi incidens esetén a Rendeletben foglalt kötelezettségeinek maradéktalanul eleget tegyen és a megfelelést utólag is igazolni tudja.

*****

Bevezetés

A személyes adat fogalma

A Rendelet 4. cikkében foglalt fogalommeghatározások 1. pontjában az alábbiak szerint rögzíti a személyes adat fogalmát:

„személyes adat": azonosított vagy azonosítható természetes személyre („érintett") vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható;"

Személyes adatnak minősül tehát minden, egy természetes személyre vonatkozó információ, amely alapján közvetve vagy közvetlenül az adott magánszemély azonosítható vagy azonosított.

Személyes adatok az egyes azonosító adatok (például név, születési hely, idő, de a személyi igazolvány szám, TAJ szám, adóazonosító jel is), a helymeghatározó adatok (pl. GPS koordináta), de például egy felhasználói fiókhoz tartozó felhasználónév is.

E körben szükséges kiemelni, hogy a személyazonosság igazolása és az azonosítás nem azonos fogalmak. Az azonosításhoz csak kivételes esetben szükséges mind a négy természetes személyazonosító adat (név, születési hely, idő, anyja neve és lakcím) megadása, a legtöbb esetben elegendő a név és a további három személyazonosító adat közül az egyik, amennyiben az az érintett azonosításához ténylegesen szükséges.

Az e-mail cím kapcsán sokszor felmerülő kérdés az email címek személyes adat minősége, különös tekintettel a „céges" e-mail címekre. Önmagukban az info@vállalkozás.com / iroda@vállalkozás.com típusú e-mail-címek nem minősülnek személyes adatnak, azonban a vezetéknév.utónév@vállalkozás.com típusú e-mail-címek már igen, hiszen ezek már önmagukban alkalmasak az adott személy azonosítására, így személyes adatnak minősülnek.

Személyes adat továbbá minden olyan információ (pl. a magasság, testsúly, hajszín, szemszín, beszélt nyelv, vagy bármely egyéb jellemző) amelyek összekapcsolásából beazonosítható valamely természetes személy (pl. ha egy adott csoportból következtetni lehet arra, kire vonatkoznak ezek a jellemzők).

A személyes adatok különleges kategóriái

A GDPR 9. cikk (1) bekezdése főszabály szerint megtiltja a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a természetes személyek egyedi azonosítását célzó genetikai és biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok kezelését.

Habár e tilalom alól vannak kivételek, melyek esetén jogszerűen kezelhetőek a különleges adatok, egy ilyen típusú adatot érintő adatvédelmi incidens kezelése különös körültekintést igényel, annak érdekében, hogy az adatkezelő az érintettet érő hátrányos hatásokat a lehető legkisebb mértékre csökkentse. Általánosságban megállapítható, hogy amennyiben az incidens különleges adatokat érint, nehezen elképzelhető, hogy az ne járjon magas kockázattal az érintettek jogaira és szabadságaira.

*****

Az adatvédelmi incidens fogalma

A Rendelet 4. cikkének 12. pontjában a következőképpen határozza meg az „adatvédelmi incidens" fogalmát:

„a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt *személyes adatok* (továbbiakban: adat, személyes adat) *véletlen vagy jogellenes* megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi"

Mi minősül tehát adatvédelmi incidesnek?

a) **„Megsemmisítés"**: az az eset, amikor az adatok egyáltalán nem vagy az adatkezelő számára nem használható formában léteznek.

Példák:

- az adatok véletlenül vagy jogellenesen (pl. arra jogosulatlan által) törlésre kerülnek,
- az adatokat tároló adathordozó megsemmisül,
- az adatokat tartalmazó papír alapú dokumentumok megsemmisülnek,
- az informatikai rendszer részének vagy egészének használhatatlanná válása vírus vagy egyéb rosszindulatú szoftver által.

b) A személyes adatok **„elvesztése”:** úgy értelmezendő, hogy az adatok még léteznek, de az adatkezelő már nem rendelkezik felettük, nem fér hozzájuk, vagy azok nincsenek a birtokában.

Példák:

- az adatokat tároló adathordozót (laptop, pendrive, céges telefon vagy akár egy papírmappa) elveszítik,
- azt ellopják,
- a személyes adatokat az adatkezelő titkosítja, de a titkosításhoz használt kulcs már nincs a birtokában,
- az eszközre történő belépéshez használt jelszó elveszik.

c) **„Megváltoztatás”**: az az eset, amikor az adatkezelő a helyes adatot kezeli, azonban az adatkezelés során valamilyen okból kifolyólag azok megváltoznak.

Példák:

- rögzített videófelvételvételből kivágásra kerül egy rész,
- a követeléskezeléskezeléshez használt szoftver meghibásodik és a tartozások összege összekeveredik.

d) A személyes adatok **közlése (vagy hozzáférhetővé tétele) arra jogosulatlan címzettek számára**:

Példák:

- személyes adatokat tartalmazó iratok, e-mail üzenetek téves címzett részére történő megküldése,
- személyes adatok jogellenes nyilvánosságra hozatala,
- személyes adatok arra jogosulatlanok részére történő hozzáférhetővé tétele (pl. e-mail küldése egymásnak ismeretlen címzettek részére úgy, hogy a címzettek megismerhetik egymás e-mail címét)

Fontos!
Az adott cselekmény incidensként való minősítését nem befolyásolja, hogy azt szándékosan vagy véletlenül követték-e el. Tehát teljes mindegy, hogy egy adathordozót véletlenül veszítettünk-e el vagy azt valaki ellopta, az eset adatvédelmi incidensnek fog minősülni.

*****

Milyen következményei lehetnek a bekövetkezett incidensnek?

Az adatvédelmi incidenseknek különféle, jelentősen hátrányos hatásai lehetnek azokra, akiknek a személyes adatát az incidens érinti.

Ezek a hatások megfelelő és kellő idejű intézkedés hiányában fizikai, vagyoni vagy nem vagyoni károkhoz vezethetnek, melyek a GDPR (85) preambulum bekezdése szerint többek között az érintettekre nézve az alábbiakat eredményezhetik:

- személyes adataik feletti rendelkezés elvesztését vagy a jogaik korlátozását,
- hátrányos megkülönböztetést,
- személyazonosság-lopást vagy a személyazonossággal való visszaélést,
- pénzügyi veszteséget,
- az álnevesítés engedély nélküli feloldását,
- a jó hírnév sérelmét,
- a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülését,
- illetve a szóban forgó természetes személyeket sújtó egyéb jelentős gazdasági vagy szociális hátrányt.

*****

Mi a teendő az adatvédelmi incidens bekövetkezése esetén?

1. Észlelés

Az adatvédelmi incidenst **elsőként érzékelő munkavállaló köteles azt azonnal jelenteni:**

- a szervezeti egysége vezetőjének,
- az adatvédelmi tisztviselőnek, valamint
- az adatkezelő adatvédelmi és adatkezelési szabályzatában megjelölt adatvédelemért felelős vezetőjének (a továbbiakban: „Felelős vezető").

A Társaság esetében az adatvédelmi és adatkezelési szabályzatban megjelölt adatvédelemért felelős vezető az Igazgatóság Elnöke.

A munkavállaló a jelentésben **röviden ismerteti az adatvédelmi incidens jellegét**, beleértve az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát.

Ezzel egyidejűleg a munkavállaló **haladéktalanul megtesz mindent annak érdekében, hogy az incidens következményeit enyhítse, a további károkat elhárítsa.**

2. Kivizsgálás, értékelés

Incidens bekövetkezése esetén a Felelős vezető az incidens körülményeinek felderítéséhez és a következmények enyhítéséhez szükséges szakértelemmel rendelkező adatvédelmi, jogi és informatikai szakértők bevonásával haladéktalanul megkezdi

- annak megállapítását, hogy valóban történt-e incidens,
- az incidens kivizsgálását és megszüntetését, továbbá
- gondoskodik a szükséges kárenyhítési intézkedések megtételéről,
- egyben értékeli az incidensnek az érintettek jogaira nézve gyakorolt hatása súlyosságát.

Az értékelés során először meg kell vizsgálni, hogy az incidens valószínűsíthetően jár-e kockázattal az egyének jogaira és szabadságaira nézve.

Fontos, hogy az adatkezelő rögtön **az incidensről való tudomásszerzést követően** ne kizárólag az incidens elhárításra törekedjen, hanem **az incidenssel járó kockázatot is felmérje.** Ennek két lényeges oka van: az egyénekre gyakorolt hatás valószínűségének és lehetséges súlyosságának ismeretében az adatkezelő egyrészről könnyebben tud hatékony intézkedéseket hozni az incidens elhárítására és kezelésére, másrészt gördülékenyebben meg tudja állapítani, hogy kell-e a Hatóságnak bejelentést tenni, és szükség esetén az érintett egyéneket értesíteni.

Az adatkezelő az egyéneket az incidens miatt érő kockázat felmérése és értékelése során figyelembe veszi annak konkrét körülményeit, köztük a lehetséges hatás súlyosságát és a bekövetkezésének valószínűségét, így különösen:

- **az incidens jellegét,**

  (Például az egyén számára eltérő következményekkel járhat a titoksértés, amelynek keretében egészségügyi információk jogosulatlan személyekhez jutnak, mint az incidens, amelynek keretében az egyén egészségügyi adatai csak hozzáférhetetlenné válnak.)

- az incidensben érintett személyes **adatok jellegét, érzékenységét és mennyiségét,**

  (Általában minél több az incidensben érintett adat, vagy azok minél érzékenyebbek, annál nagyobb a kár bekövetkeztének kockázata az érintett egyének számára.

  Az egészségügyi adatokat, személyazonosító okmányokat vagy pénzügyi adatokat, például hitelkártya adatokat érintő incidensek önmagukban is mind kárt okozhatnak, együttesen azonban személyazonosság-lopáshoz vezethetnek. A személyes adatok rendszerint együttesen érzékenyebbnek tekinthetők, mint külön-külön, sőt olyan eset is előfordulhat, hogy önmagukban nem személyes adatnak minősülő adatok együtt már azonosítható tesznek valaki, és így személyes adatoknak minősülnek.)

- az **egyének könnyű azonosíthatóságát,**

  (Fontos, mérlegelendő tényező, hogy a veszélyeztetett személyes adatokhoz hozzáférő fél mennyire könnyen tudja azonosítani az egyes egyéneket, vagy egyének azonosítása céljából más információkkal összeegyeztetni az adatokat.)

- az egyéneket érintő **következmények súlyosságát,**

  (Például különleges kategóriájú adatok esetében különösen súlyosak lehetnek az egyéneket fenyegető lehetséges károk, különösen akkor, ha az incidens személyazonosság-lopáshoz, személyazonossággal való visszaéléshez, a becsület csorbításához vagy hírnév rontáshoz vezethet.

  Az egyéneket érintő következmények tartósságát is mérlegelni kell, mivel általánosságban hosszan tartó hatások esetén súlyosabb az incidens kihatása.)

- az **egyén sajátosságait,**

  (Az incidens érintheti gyermekek vagy más olyan, kiszolgáltatott helyzetben lévő egyének személyes adatait, akik ennek következtében nagyobb veszélybe kerülhetnek.)

- az **adatkezelő sajátosságait,**

(Például az egészségügyi szervezetek különleges kategóriájú személyes adatokat dolgoznak fel, következésképpen e személyes adataik megsértése esetén nagyobb fenyegetés éri az egyéneket.)

- az érintett **egyének számát,**

  (Általánosságban minél nagyobb az érintett egyének száma, annál nagyobb negatív hatást gyakorol az incidens.)

- további általános, illetve az incidens természetéből adódó olyan szempontokat, melyek segíthetnek annak eldöntésében, hogy szükséges-e bejelentést tenni, illetve szükséges-e tájékoztatni az érintetteket.

Fontos! Ha bármilyen alacsony kockázat is fennáll egy adott incidenssel kapcsolatban, a kockázat hiányának valószínűsíthetőségétől nem lehet beszélni. Ha az incidenssel kapcsolatban minden releváns tényező nem állapítható meg, akkor a kockázatok és azok bekövetkezése valószínűségének feltárásához sem állhatnak rendelkezésre a szükséges adatok, a kockázat nem zárható ki, és annak kizártsága sem valószínűsíthető ilyen helyzetben.

A kivizsgálás során meg kell bizonyosodni arról, hogy az összes megfelelő technológiai védelmi és szervezési intézkedés végrehajtásra került-e, egyrészt az adatvédelmi incidens bekövetkezte és következményeinek haladéktalan megállapítása, másrészt a felügyeleti hatóságnak történő bejelentés és az érintett sürgős értesítése érdekében.

3. Bejelentés a Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: NAIH vagy Hatóság) felé

Az adatvédelmi incidenst az Adatkezelő **indokolatlan késedelem nélkül, a tudomására jutástól számított 72 órán belül köteles bejelenteni a Hatóságnak.**

Mikor jut az adatvédelmi incidens az adatkezelő „tudomására"?

Akkor tekinthető úgy, hogy az incidens az adatkezelő „tudomására" jutott, **amikor az adatkezelő észszerű bizonyossággal meggyőződött arról, hogy olyan biztonsági incidens történt, amelynek következtében a személyes adatok veszélybe kerültek.**

A GDPR kimondja, hogy azt, hogy a bejelentésre indokolatlan késedelem nélkül került-e sor, különösen az adatvédelmi incidens jellegére és súlyosságára, valamint annak az érintettre gyakorolt következményeire, illetve hátrányos hatásaira figyelemmel kell megállapítani. Ezzel kötelezettséget ír elő az adatkezelő számára a tekintetben, hogy időben szerezzenek „tudomást" az esetleges incidensekről, mivel így tudják megtenni a megfelelő intézkedést.

Az incidens körülményeitől függ, pontosan mikor tekinthető úgy, hogy az incidens az adatkezelő „tudomására" jutott. Bizonyos esetekben már kezdettől fogva viszonylag egyértelmű, hogy incidens történt, míg máskor némi időbe telhet annak megállapítása, hogy a személyes adatok sérültek. **A lényeg** azonban, hogy **gyorsan ki kell vizsgálni incidenst annak megállapítása érdekében, hogy valóban sérültek-e a személyes adatok, és ha igen, korrekciós intézkedéseket hozni, és szükség esetén bejelentést kell tenni.**

Példák:

- Titkosítatlan személyes adatokat tartalmazó adathordozó elvesztése esetén gyakran nem lehet meggyőződni arról, hogy jogosulatlan személyek hozzáfértek-e az adatokhoz. Mindazonáltal, még ha az adatkezelő nem is tudja megállapítani, hogy sérült-e az adatok bizalmas jellege, az incidenst akkor is be kell jelenteni, mivel észszerű bizonyossággal feltételezhető, hogy sérült a hozzáférhetőség. Az adatkezelőnek ez az eset akkor jut „tudomására", amikor fény derül arra, hogy az adathordozó elveszett.
- Harmadik fél arról tájékoztatja az adatkezelőt, hogy véletlenül az adatkezelő tevékenysége következményeként a birtokába jutottak az adatkezelő egyik ügyfelének személyes adatai, és a jogosulatlan közlést bizonyítékkal is alátámasztja. Mivel az adatkezelő egyértelmű bizonyítékot kapott a tekintetben, hogy sérült az adatok bizalmas jellege, így kétségtelenül a „tudomására" jutott az incidens.
- Az adatkezelő észleli, hogy lehetséges, hogy behatoltak az informatikai hálózatába. Ellenőrzi rendszereit annak megállapítása érdekében, hogy a bennük tárolt személyes adatok sérültek-e, és adott esetben ezt megállapítja. Az adatkezelőnek ez esetben is egyértelmű bizonyítéka van az incidens megtörténtére, így kétségtelenül a „tudomására" jutott az incidens.

Van-e kivétel a bejelentési kötelezettség alól?

Akkor nem szükséges bejelenteni a Hatósághoz az adatvédelmi incidenst, ha az valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve.

A fenti 2. pontban foglaltak szerint ez a kivétel azonban szűken értelmezendő!

Példa:

- Amikor a személyes adatok már egyébként is nyilvánosan hozzáférhetőek, és az ilyen adatok közlése valószínűleg nem jelent kockázatot az egyén számára.
- Bejelentést nem igénylő incidens lehet továbbá az adatkezelő és alkalmazottai által használt, biztonságosan titkosított mobilkészülék elvesztése. Amennyiben a titkosítási kulcs biztonságosan továbbra is az adatkezelő birtokában van, és nem a készüléken volt a személyes adatok egyetlen példánya, akkor ezekhez az adatokhoz semmilyen támadó nem tud hozzáférni. Következésképpen az incidens valószínűsíthetően nem jár kockázattal a kérdéses érintettek jogaira és szabadságaira nézve. Ha később nyilvánvalóvá válik, hogy a titkosítási kulcs veszélybe került, illetve a titkosító szoftver vagy algoritmus sebezhető, akkor a természetes személyek jogait és szabadságait érintő kockázat megváltozik, így már szükség lehet bejelentésre.

A bejelentés megtétele, tartalma

A bejelentés a Hatóság weboldalán keresztül (https://www.naih.hu/adatvedelmi-incidensbejelent--rendszer.html) elektronikus formában tehető meg.

A bejelentés megtétele az adatvédelmi tisztviselő közreműködésével a Felelős vezető kötelezettsége.

A GDPR 33. cikk (3) bekezdése rögzíti, hogy amikor az adatkezelő bejelentést tesz incidensről a Hatóságnak, abban legalább:

a) **ismerteti az adatvédelmi incidens jellegét**, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát;
b) **közöli az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartónevét és elérhetőségeit;**
c) **ismerteti** az adatvédelmi incidensből eredő, valószínűsíthető **következményeket;**
d) **ismerteti** az adatkezelő által az adatvédelmi incidens **orvoslására tett vagy tervezett intézkedéseket,** beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányoskövetkezmények enyhítését célzó intézkedéseket.

Az, hogy a 33. cikk (3) bekezdése kimondja, hogy az adatkezelőnek „legalább" a megjelölt információkat kell közölnie a bejelentésben azt jelenti, hogy szükség szerint dönthet úgy, hogy további részleteket ad meg, sőt, minden esetben javasolt, hogy az adatkezelő minden rendelkezésre álló információt adjon át a Hatóság részére. Előfordulhat, hogy eltérő jellegű incidensek előfordulása estén további információkkal kell szolgálni mindegyik esetkörülményeinek maradéktalan ismertetéséhez.

A Hatóság minden esetben jogosult az incidens kivizsgálása során részletesebb felvilágosítást kérni.

Bejelentés részletekben

Az incidens jellegétől függően előfordulhat, hogy az adatkezelőnek további vizsgálatot kell lefolytatnia az incidens szempontjából lényeges összes tény megállapítása céljából.

A 33. cikk (4) bekezdése ezért a következőképpen rendelkezik:

„Ha és amennyiben nem lehetséges az információkat egyidejűleg közölni, azok további indokolatlan késedelem nélkül később részletekben is közölhetők."

Az adatkezelő nem mindig rendelkezik az incidensről való tudomásszerzéstől számított 72 órán belül az összes szükséges információval, ugyanis nem minden esetben állnak rendelkezésre maradéktalan és minden részletre kiterjedő adatok az incidensről ebben a kezdeti időszakban. A rendelet ezért megengedi a részletekben történő bejelentést abban az esetben, ha az adatkezelő a 33. cikk (1) bekezdésében foglaltak szerint **megindokolja a késedelmet**.

Mit kell ez esetben az első bejelentésnél közölni a Hatósággal?

Amikor az adatkezelő a részletekben történő bejelentés során első alkalommal tesz bejelentést a Hatóságnak, mindig tájékoztatást kell adnia arról, ha még nem rendelkezik az összes szükséges információval és a későbbiekben fog tudni további részleteket közölni. Az adatkezelő kiegészítő információkkal szolgálhat akkor, amikor olyan további lényeges adatok jutnak a tudomására, amelyeket relevánsak az ügyben.

Példa: Az adatkezelő az adatvédelmi incidens észlelésétől számított 72 órán belüli bejelentést tesz a NAIH-nak arról, hogy elveszítette az egyes ügyfelei személyes adatainak másolatát tartalmazó adathordozót. Később kiderül, hogy az adathordozót rossz helyre tették az adatkezelő helyiségein belül, így végül megkerül. Az adatkezelő tájékoztatja a felügyeleti hatóságot ennek tényéről és módosítja a bejelentést.

Mi a teendő késedelmes bejelentés esetén?

Ha a bejelentés nem történik meg 72 órán belül, a határidőn túl megtett bejelentéshez **mellékelni kell a késedelem igazolására szolgáló indokokat is.**

Késedelmes bejelentésre csak kivételes, indokolt esetben kerülhet sor, a késedelem indokát pedig a Hatóság tudomására kell hozni. Nem lehet például arra hivatkozni, hogy a bejelentésre azért került késedelmesen sor, mert a bejelentésért felelős munkavállaló éppen szabadságon volt.

Közölhető-e több hasonló incidens egy bejelentésben?

Szigorúan véve minden egyes adatvédelmi incidens bejelentendő. Azonban a túlzott terhelés elkerülése érdekében az adatkezelő benyújthat az összes incidensre vonatkozó, „összevont" bejelentést, feltéve, ha az incidensek viszonylag rövid időn belül ugyanolyan módon megsértett, azonos jellegű személyes adatokat érintenek.

Ha sorozatosan következnek be olyan incidensek, amelyek különböző módon megsértett, eltérő jellegű személyes adatokat érintenek, akkor a bejelentést a szokott módon kell megtenni, tehát mindegyik incidenst külön kell jelenteni.

4. Az érintettek tájékoztatása

Az adatkezelő bizonyos esetekben a Hatóságnak való bejelentés mellett az érintett egyéneket is tájékoztatnia kell az adatvédelmi incidensről.

A GDPR 34. cikk (1) bekezdése szerint:

„Ha az adatvédelmi incidens **valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve,** az adatkezelő **indokolatlan késedelem nélkül tájékoztatja az érintettet az adatvédelmi incidensről.**"

Mikor kell az érintetteket tájékoztatni?

A GDPR (86) preambulumbekezdés az alábbiakat rögzíti:

„Az érintettek tájékoztatásáról **az észszerűség keretei között a lehető leghamarabb gondoskodni kell,** szorosan együttműködve a Hatósággal, és betartva az általa vagy más érintett hatóságok, például bűnüldöző hatóságok által adott útmutatást."

Mit kell tartalmaznia a tájékoztatásnak?

Az érintettnek nyújtott tájékoztatás legalább az alábbi információkat tartalmazza:

- az incidens jellegének leírása;
- az adatvédelmi tisztviselő vagy egyéb kapcsolattartó neve és elérhetőségei;
- az incidens valószínűsíthető következményeinek ismertetése, valamint
- az adatkezelő által az incidens orvoslására tett vagy tervezett intézkedések ismertetése, beleértve adott esetben az incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket is.

Az adatkezelő adott esetben konkrét tanácsokkal láthatja el az érintetteket, hogy védekezni tudjanak az incidens esetleges hátrányos következményeivel szemben, például javasolhatja, hogy állítsanak be maguknak új jelszót, amennyiben hozzáférési hitelesítő adataik kerültek veszélybe, vagy tiltsák le a bankkártyájukat, amennyiben annak adatai kompromittálódtak. Az adatkezelő ez esetben is javasolt, hogy az előírt minimumnál bővebb tájékoztatást nyújtson.

Milyen formában történhet a tájékoztatás?

Fontos!
Az érintettek incidensről **való tájékoztatásához kifejezetten erre vonatkozó üzeneteket kell alkalmazni,** amelyek **nem küldhetők más jellegű tájékoztatással,** például az aktualitásokról szóló rendszeres értesítésekkel, hírlevelekkel vagy szabványüzenetekkel együtt. Az incidensről való tájékoztatás ezáltal egyértelmű és átlátható lesz.

Az adatkezelő az incidensről szóló tájékoztatást tömör, átlátható, érthető és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazva nyújtja, különösen a gyermekeknek címzett bármely információ esetében. Az információkat írásban vagy más módon – ideértve adott esetben az elektronikus utat is – kell megadni, megfelelve a GDPR 5. cikk (2) bekezdésében írt elszámoltathatóság követelményének.

Átlátható tájékoztatási módszer például

- a közvetlen üzenetküldés (például e-mail, SMS, közvetlen üzenet),
- a honlapon kiemelt helyen megjelenített szalaghirdetés vagy értesítés,
- a postai úton történő tájékoztatás,
- valamint a nyomtatott sajtóban megjelenő kiemelt hirdetés.

Mindig olyan megoldást kell választani, amellyel a legnagyobb az esély arra, hogy minden érintett egyént megfelelően tájékoztatnak. A körülményektől függően az is elképzelhető, hogy az adatkezelőnek többféle tájékoztatási eszközt is igénybe kell vennie, ahelyett, hogy egyetlen kapcsolattartási csatornára hagyatkozna.

Mikor mellőzhető az értesítés?

A GDPR 34. cikk (3) bekezdése határozza meg azt a három feltételt, amelynek teljesülése esetén **nem szükséges értesíteni az egyéneket** incidens bekövetkezésekor.

Ezek a feltételek az alábbiak:

a) az adatkezelő **megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre,** és ezeket az intézkedéseket az adatvédelmi incidens által érintett adatok tekintetében alkalmazták, különösen azokat az intézkedéseket – mint például a titkosítás alkalmazása –, amelyek a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik az adatokat;

Ilyen intézkedés például a személyes adatok legkorszerűbb titkosítással (jelszóval) történő védelme, melyet egyébként a Hatóság is elvár az adatkezelőktől. Az adatok titkosítására vonatkozó kötelezettség érintheti a hordozható eszközöket, irodai eszközöket, okostelefonokat, de érzékeny, vagy nagy számú adat e-mailben történő küldése során is szükséges az adatok jelszóval történő védelme, ezzel megelőzve, hogy félreküldés esetén illetéktelenek ismerhessék meg az adatokat.

b) az adatkezelő az **adatvédelmi incidenst követően olyan további intézkedéseket tett,** amelyek biztosítják, hogy az érintett jogaira és szabadságaira jelentett magas kockázat a továbbiakban valószínűsíthetően nem valósul meg;

Az eset körülményeitől függően például előfordulhat, hogy az adatkezelő azonnal azonosította azt az egyént, aki az adatokhoz hozzáférhet és azonnal, mielőtt még az adatok felhasználására e személynek lehetősége lenne, megtette a szükséges intézkedéseket.

c) a tájékoztatás **aránytalan erőfeszítést tenne szükségessé.**

Például azért, mert elérhetőségi adataik az incidens következtében elvesztek, vagy eleve nem is voltak ismertek.

Például egy raktárt elönt a víz, és a személyes adatokat tartalmazó dokumentumok megsemmisültek, azokat azonban kizárólag papíralapon tárolták.

Az adatkezelőnek azonban **ilyenkor nyilvánosan közzétett információk útján kell tájékoztatnia** az egyéneket, vagy olyan hasonló intézkedést kell hoznia, amely biztosítja a hasonlóan hatékony tájékoztatásukat.

A nyilvános tájékoztatás megtehető például a Társaság honlapján, vagy az érintett által használt applikációban, a fent említettek szerint például egy szalaghirdetéssel a honlap kezdőlapján vagy egy, az applikációban minden felhasználó részére tett értesítéssel.

Az elszámoltathatósági elvnek megfelelően, amennyiben az adatkezelő nem értesíti az érintetteket, **tudnia kell bizonyítani** a Hatóság felé, **hogy e feltételek közül egynek vagy többnek megfelel, ezért is kiemelten fontos, hogy az incidenssel kapcsolatos minden körülmény írásban kerüljön rögzítésre.** Ha a Hatóság megállapítja, hogy az érintettek értesítésének mellőzésére vonatkozó döntés nem megalapozott, akkor élhet a rendelkezésére álló hatáskörrel és szankciókkal.

Szem előtt kell tartani, hogy kezdetben talán nem szükséges bejelentést tenni vagy tájékoztatást adni, ha nincs a természetes személyek jogait és szabadságait érintő kockázat, ez azonban idővel változhat, és előfordulhat, hogy újra fel kell mérni a kockázatot. Az adatkezelő tehát folyamatosan értékeli az incidens kivizsgálása során tudomására jutó új információkat, és amennyiben szükséges, akár időközben módosít az addigi incidens-kezelési stratégiáján.

5. Az incidens nyilvántartása

Az elszámoltathatóság elvével összefüggésben az adatkezelő köteles nyilvántartani a bekövetkezett adatvédelmi incidenseket, feltüntetve az adatvédelmi incidenshez kapcsolódó fontosabb tényeket, körülményeket az alábbiak szerint:

a) időpont;
b) incidens leírása;
c) incidens hatása az érintettekre;
d) érintettek száma;
e) érintettek kategóriái;
f) érintett személyes adatok köre, száma;
g) incidens következményei;

h) incidens következményeinek orvoslására tett intézkedések;
i) érintettek tájékoztatása megtörtént-e, és ha igen, mikor.

Az adatkezelő a bejelentési kötelezettség alá tartozó incidensek mellett **a bejelentési kötelezettség alá nem tartozó incidensekről is** nyilvántartást vezet. **Ha az adatkezelő úgy ítéli meg, hogy az incidenst nem kell bejelentetni, úgy e döntése indoklását is nyilvántartja**. Az indoklás tartalmazza azokat az okokat, amikre alapozva az adatkezelő úgy ítéli meg, hogy az incidens valószínűsíthetően nem jár kockázattal az egyének jogaira és szabadságaira nézve.

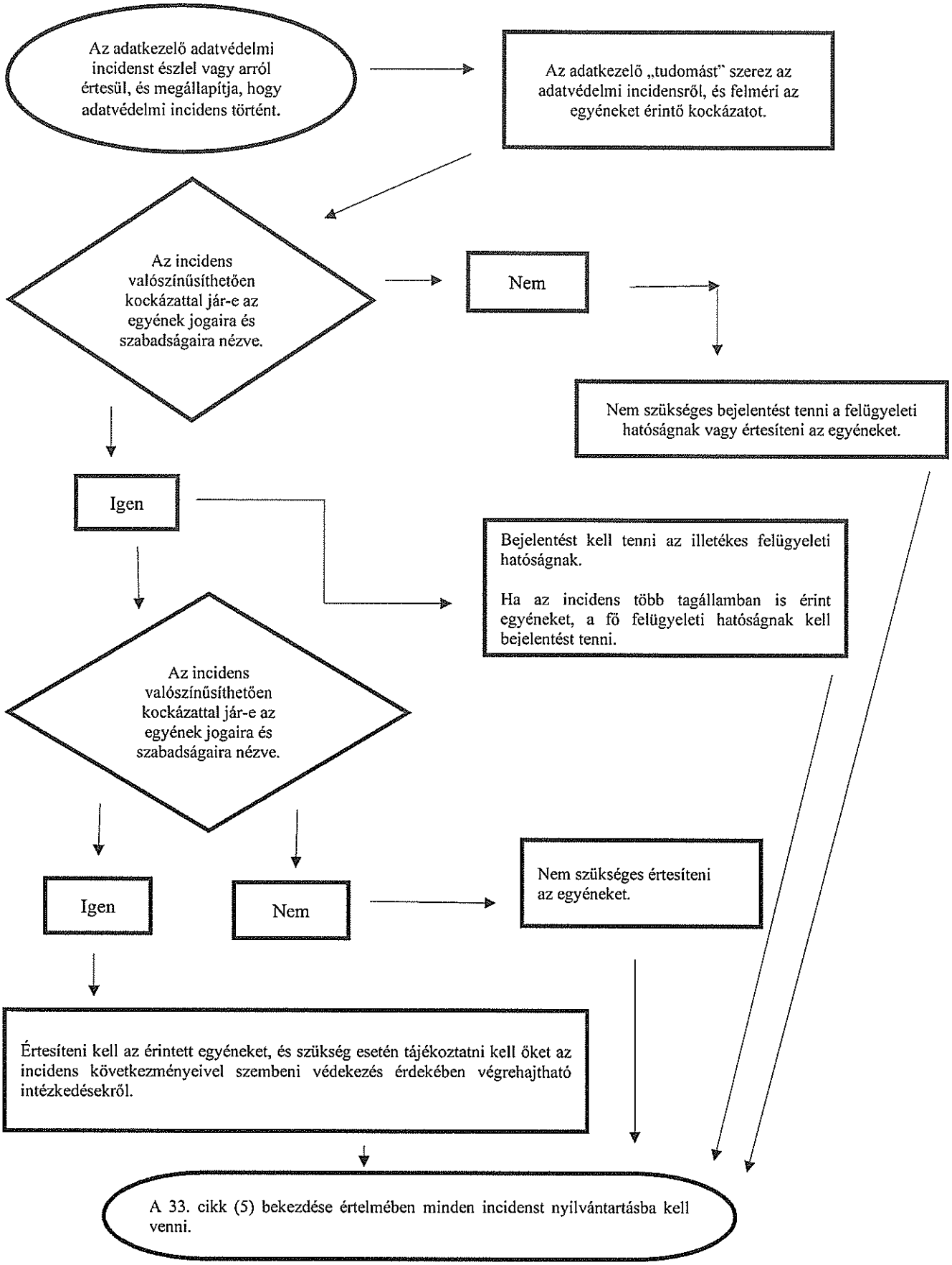
Pécs, 2019. december 13.

Tüke Busz
Közösségi Közlekedési
Zártkörűen Működő Részvénytársaság
7634 Pécs, Nyugati ipari út 8.
Adószám: 23071067-2-02 1.

Tüke Busz Közösségi Közlekedési Zártkörűen Működő Részvénytársaság
Képv.: Gelencsér Gyula Igazgatóság Elnöke

Melléklet: Folyamatábra a bejelentési kötelezettségről

Folyamatábra a bejelentési kötelezettségről



Forrás: A 29. cikk szerinti adatvédelmi munkacsoport iránymutatása az adatvédelmi incidensek (EU) 2016/679 rendelet szerinti bejelentéséről