SALUS VOCALIS. Csegöldi indulás - Győri érkezés.
DOI: 10.59199/salusvocalis.2023.69

WELLMANN BARNA BENCE
egyetemi tanársegéd
SZE Deák Ferenc Állam- és Jogtudományi Kar

Az adatvédelmi incidensről tíz oldalban

ABSZTRAKT

Amennyiben az adatkezelőre irányadó adatbiztonsági elvárások olyan sérüléséről van szó, 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, úgynevezett adatvédelmi incidensről beszélünk. 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, a hátrányos megkülönböztetést, a személyazonosság-lopást vagy a személyazonossággal való visszaélést, a 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. Vagyis az ilyen helyzetek megelőzése, elhárítása és megfelelő kezelése kulcsfontosságú. Jelen tanulmány célja az adatvédelmi incidensekhez kapcsolódó szabályanyag rövid és összefoglaló jellegű bemutatása.

Kulcsszavak: adatbiztonság ■ adatvédelem ■ adatvédelmi incidens ■ jogkövetkezmények

I. BEVEZETÉS

A regionális adatvédelmi jog GDPR[1] által rögzített alapelvei között nevesített ún. integritás és bizalmas jelleg elve kimondja, hogy az adat-

[1] Az Európai Parlament és a Tanács (EU) 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 rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) (General Data Protection Regulation, a továbbiakban: GDPR vagy Rendelet).

kezelőnek, illetve az adatfeldolgozónak „a személyes adatok kezelését oly módon kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve".[2] Azt, hogy ennek részeként pontosan milyen mértékű védelmet is kell biztosítani, több szempont is befolyásolja, befolyásolhatja. Egyrészről ide sorolható a tudomány és technológia állása, amely azt a kötelezettséget generálja az adatkezelő felé, hogy kísérje figyelemmel az elérhető és modern preventív/defenzív technikákat, és ne alkalmazzon elavult védelmi mechanizmust.[3] Másrészről az adatkezelés általános körülményei, céljai, hatóköre, illetve ezeknek az adatalany magánszférájára gyakorolt kockázatai is befolyással vannak az alkalmazandó védelem mértékére, hiszen más biztonsági szabályokat kell alkalmazni például akkor, ha az adatkezelés célja az érintett egészségügyi állapotának részletes feltérképezése, és mást, ha az adatkezelés célja mondjuk az érintettektől elégedettségi kérdőívek begyűjtése.

Amennyiben az adatkezelő ezeknek az elvárásoknak akár tudatosan, akár gondatlanságból nem tesz eleget, azoknak nem felel meg az eljárása, intézkedése, az általa kezelt személyes adatok veszélybe kerül(het)nek, a védelmük és biztonságuk sérül. Ha pedig a biztonság olyan sérüléséről van szó, „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," úgynevezett adatvédelmi incidensről beszélünk.[4]

II. AZ ADATVÉDELMI INCIDENSEK TERMÉSZETE

A fenti definíció ellenére jómagam úgy vélem, hogy nincsen feltétlenül szó minden esetben káros következményről, nem tartom az adatvédelmi incidens szükségszerű velejárójának a személyes adatok tényleges sérelmét. Megítélésem szerint valójában csak az adatbiztonságnak, azaz az adatok védelmét szolgáló technikai és szervezési intézkedéseknek a sérelmét takarja az intézmény, s ehhez csak (gyakori, de nem törvényszerű) járulékos következményként társul a sérelem, mint eredmény. E felvetésemet a Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: NAIH vagy Hatóság) 2019/2471. számú határozata is alátámasztja. E döntésben a Hatóság kimondta, hogy a személyes adatokat tartalmazó, megfelelő védelmet nélkülöző pendrive elveszítése „önmagában is kockázatos adatvédelmi incidenst eredményez, akkor is, ha egyéb-

[2] GDPR 5. cikk (1) bekezdés f) pont.

[3] Vö.: Győrffyné Holló, 2021, 17-23.

[4] GDPR 4. cikk 12. pont és az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) 3. § 26. pont.

ként az azokhoz való jogosulatlan hozzáférés, nyilvánosságra hozatal, vagy az adatokkal való egyéb visszaélés ténye nem is állapítható meg".[5] Tehát a NAIH a lehetséges jogosulatlan hozzáférést is kockázatként értékelte, elismerve, hogy tényleges eredmény nélkül, pusztán a sérelem reális veszélye is megalapozhatja az adatvédelmi incidens megállapítását.[6]

Az adatvédelmi incidensek megelőzése és elhárítása érdekében az adatkezelő különböző szervezési, illetve technikai intézkedéseket köteles tenni.[7] A szervezési intézkedések nem mást takarnak, mint azokat a belső, az adatkezelő szervezetére irányadó eljárásrendi szabályokat, amelyek meghatározzák az adatvédelmi követelmények (ezen belül is jelen témakör szempontjából az adatbiztonság) érvényesülését és érvényesítését szolgáló normatív jellegű előírásokat. Ilyenek tipikusan maguk az adatkezelési szabályzatok, vagy az adatkezelő által meghatározott adatvédelmi protokollok, infrastrukturális elvárások. Vagyis ezek azok a dokumentumok, amelyek átültetik a gyakorlatba és konkrét tartalommal töltik meg az egyes adatvédelmi alapelvek és a jogszabályok által megfogalmazott elvárásokat.[8] Ehhez képest a technikai intézkedések a szervezési intézkedések végrehajtását, illetve az adatbiztonsági gyakorlatoknak a mindennapi alkalmazását és érvényesítését biztosítják.[9] A működtetés biztonsága ráadásul az emberi tényezőn (is) múlik, vagyis azon, hogy az e rendszerekhez kapcsolódó eszközöket kezelő, használó, azokhoz hozzáférő személyek jogosultságaikat csak kellő szakismerettel és óvatossággal, a meghatározott körben és biztonsági szabályoknak megfelelően gyakorolják.[10]

Visszautalva az adatvédelmi incidens definíciójára, az intézmény szabályai és következményei akkor alkalmazandók, ha az adatbiztonság sérülése következik be. Ennek értelmében akkor esik meg adatvédelmi incidens, ha a különböző adatbiztonsági intézkedések sérülésével, megsértésével, kijátszásával az érintett személyes adatok veszélybe kerülnek. Így, ha nincs szó az adatbiztonság sérüléséről, hiába kerülnek veszélybe vagy szenvednek ténylegesen is sérelmet a személyes adatok, az eset kívül esik az adatvédelmi incidens értékelési körén.[11]

Párhuzamba állítva azzal a ténnyel, hogy az adatkezelést megvalósító cselekmények, illetve maguk a személyes adatok is gyakorlatilag kimeríthetetlen listát alkotnak, a lehetséges adatvédelmi incidensek köre is lényegében végtelen halmazt képez. Éppen ezért nem is teszek kísérletet arra, hogy részletes felsorolásokba bocsátkozzak, ehelyett a valóban tipikus, a mindennapi életben is minden további nélkül bárkivel előforduló esetek bemutatására helyezem a hangsúlyt, melyhez a NAIH 2018. évi tevékenységéről készült beszámolót hívom segítségül.

[5] NAIH/2019/2471/6., 7. oldal.
[6] Vö. pl. NAIH-1881-5/2013/H.
[7] Vö. GDPR 5. cikk (1) bekezdés f) pont.
[8] Árvay, 2018, 211.
[9] Árvay, 2018, 212.
[10] Mayer – Verebics, 2002, 22.
[11] Ld. Buday-Sántha, 2019.

Ezek alapján a hazai gyakorlat az alábbi négy fő csoportba sorolja a leggyakoribb adatvédelmi incidenseket:

- A téves címzés miatti félrepostázások, illetve téves címzett részére küldött elektronikus levelek;
- e-mailek küldése több címzett részére oly módon, hogy a címzettek nem a „Titkos másolat", hanem a „Másolatot kap" mezőben vannak felsorolva, tehát minden címzett látja, jogosulatlanul megismeri a többi e-mail címet;
- az adatkezelőt ért támadás következtében kiszivárgott, megszerzett adatok; végül
- ellopott/elvesztett számítástechnikai eszközök, telefonok.[12]

III. AZ ADATVÉDELMI INCIDENSEK SÚLYOZÁSA

Habár az intézmény elnevezéséből pont, hogy nem vezethető le, az adatvédelmi incidensek körét mégis lehetséges, sőt szükséges is a jogsérelem (potenciális) mértéke, a hátrányos következmények súlya alapján kategorizálni, rangsorolni. Ugyanis a felemerült incidensek súlya, azaz a lehetséges jogsérelem mértéke alapján differenciált a követendő eljárás, az adatkezelőt (adatfeldolgozót) terhelő kötelezettségek sora.

Az incidens értékelési folyamata két részre bontható: első lépésként, az adatvédelmi incidens felismerésekor, az adatkezelő haladéktalanul felméri a veszély mértékét, értékeli a kockázatokat, majd az ekkor rendelkezésére álló információk birtokában, alapvetően saját mérlegelése szerint dönt az eset súlyosságáról és a követendő eljárásról. A cezúra másik oldalán maga az adatvédelmi hatóság és az ő eljárása áll, amelynek keretein belül a szerv esetleges hatósági vizsgálat útján tárja fel az eset összes körülményeit, majd ennek eredményei alapján igazolja, illetve adott esetben felülbírálja az adatkezelő minősítését, szükség esetén pedig egyéb jogkövetkezményeket is alkalmaz.

Annak érdekében azonban, hogy e minősítések mindig összhangban álljanak az uniós jogalkotói elvárásokkal, továbbá, hogy ne legyen mérhető különbség az egyes tagállamok incidenselbírálási gyakorlata között, az Európai Uniós Kiberbiztonsági Ügynökség *(European Union Agency for Cybersecurity – ENISA*[13]*)* kidolgozta az adatvédelmi incidensek súlyosságának beazonosításához szükséges

[12] A Nemzeti Adatvédelmi és Információszabadság Hatóság Beszámolója a 2018. évi tevékenységéről, 2019.

[13] Az ENISA mozaikszó az szervezet eredeti elnevezésére (European Network and Information Security Agency) vezethető vissza, melyet az Európai Parlament és a Tanács az Európai Hálózat- és Információbiztonsági Ügynökség létrehozásáról szóló 460/2004/EK rendelete (2004. március 10.) hozott létre.

iránymutatását[14] (a továbbiakban: Ajánlás).

Habár jelen tanulmány keretein belül e súlyozási képlet részletes kibontására terjedelmi okokból kifolyólag nem kerülhet sor, azt mindenképpen szükséges felvázolni, hogy az adatvédelmi incidens súlyosságát annak három különböző szempontból történő értékelésének együtteseként, eredményeként azonosíthatjuk be. E három szempont a következő:

- Az érintett adatok körét, típusát és az érintetteket, valamint az adatkezelés teljes folyamatát, céljait, eszközeit és módját feltáró ún. adatkezelési kontextus *(Data Processing Context – DPC).*
- Az azonosítás egyszerűsége *(Ease of Identification – EI),* amely annak vizsgálatát és mérlegelését követeli meg, hogy az adatvédelmi incidenssel érintett konkrét adatokból mennyire könnyen lehet következtetni az érintettre, azok milyen eséllyel alkalmasak arra, hogy – közvetlenül vagy közvetve – azonosíthatók legyenek az egyes egyének.
- Végül pedig az incidens körülményei *(Circumstances of Breach – CB)*, amely a már bekövetezett adatvédelmi incidens egyedi körülményeinek feltárására irányul. Ennek során az adatkezelő a biztonságban bekövetkezett sérülések (azaz a védelmi szint csökkenésének), illetve az incidens mögött esetlegesen meghúzódó felróhatósági elem feltárására köteles.

A fenti három kategórián belül különböző minősítő tényezők jelennek meg, mely faktorokhoz különböző értékelési pontszámok tartoznak. E pontszámok egy pontozási művelet elvégzéséhez szükségesek, melynek eredménye fogja megadni az egyes konkrét adatvédelmi incidens úgynevezett SE *(Severity* vagy *Severity Level)* értékét, vagyis az adott eset tényleges veszélyességi indexét. Az így kapott érték pedig egy négyfokozatú skála alapján determinálja a bekövetkezett adatvédelmi incidens súlyosságát, ezáltal pedig a követendő eljárásokat és a lehetséges jogkövetkezményeket is. Ez az egyenlet a következő:

$$SE = DPC \times EI + CB$$

Az így kapott érték az Ajánlás által kidolgozott táblázat alapján beazonosíthatóvá teszi az adatvédelmi incidens súlyosságát, az alábbiak szerint:

[14] Manso – Górniak, 2013

SE-index	Veszélyességi besorolás	Az incidens lehetséges hatásai
0 ≤ SE < 2	Alacsony	Az érintetteket egyáltalán nem éri hátrány, illetve sérelem, vagy csupán olyan kellemetlenséggel szembesülhetnek, melyek gond nélkül elháríthatók, orvosolhatók. Pl.: az adatok újbóli rögzítésének szükségessége, megnövekedett ügyintézési idő stb.
2 ≤ SE < 3	Közepes	Az érintettek jelentősebb kellemetlenségekkel szembesülhetnek, azonban ezeket kisebb nehézségek, többletteljesítmények árán orvosolni lehet. Pl.: az incidenssel összefüggésben felmerülő többletkiadások megjelenése, szolgáltatások igénybe vételének visszautasítása, pszichés megterhelés (stressz, félelem) stb.
3 ≤ SE < 4	Magas	Az érintettek jelentős következményekkel találhatják szemben magukat, melyek elhárításához, illetve orvoslásához komoly erőfeszítéseket kell tenniük. Pl.: vagyoni és nem vagyoni károk megjelenése, egészségromlás, munkaviszony megszüntetése stb.
4 ≤ SE	Nagyon magas	Az adatvédelmi incidens az egyénekre nézve lényegében elháríthatatlan, illetve visszafordíthatatlan következményekkel jár. Pl.: az érintett halála, magáncsőd bekövetkezte, munkaképesség elvesztése, tartós lefolyású megbetegedések kialakulása stb.

1. táblázat: Az adatvédelmi incidensek veszélyességi besorolása
(Forrás: saját szerkesztés, az Ajánlás 3.2. pontja alapján)

E számítási metódust és minősítési kategóriákat azonban nem feltétlenül találjuk meg a hazai gyakorlatban, hiszen a Hatóság és a jogalkotó is elsődlegesen három kategóriában gondolkozik: a főszabály szerinti középérték, valamint az ehhez képest alacsony, illetve magas veszélyességi szintekben. Természetesen a „Nagyon Magas" veszélyességi kategória része a magas veszélyszintnek, így végülis annak hiánya nem problematikus. Persze, az is tényszerűen kijelenthető, hogy a hazai jogrendszer minőségi szintjeit is szükséges valamilyen értékelési rendszerhez kötni, ezért – még akkor is, ha mindez csupán ajánlási szinten, azaz normatív erővel nem bíró módon került meghatározásra – ahhoz jómagam az Ajánlás által kidolgozott rendszer követését javaslom.

IV. AZ ADATVÉDELMI INCIDENS KÖZVETLEN KÖVETKEZMÉNYE – A BEJELENTÉSI KÖTELEZETTSÉG

„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, a hátrányos megkülönböztetést, a személyazonosság-lopást vagy a személyazonossággal való visszaélést, a 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."[15]

Az előbbi idézetből is egyértelműen kiderül, hogy az adatvédelmi incidens akár rendkívül komoly hátrányok, sérelmek kiváltó oka is lehet. Mindez szükségessé teszi, hogy az adatkezelők mindig megfelelő időben és módon tudják kezelni a személyes adatokat érő váratlan helyzeteket, adatvédelmi incidenseket. A gyakorlati életben ugyanis sem a felügyeleti szervek, sem pedig az egyes érintett egyének nincsenek mindig tisztában azzal, hogy éppen adatvédelmi incidens merült-e fel, illetve adott esetben annak sértettjeivé váltak. Így értelemszerűen azokra reagálni, saját védelmük érdekében a szükséges lépéseket megtenni sincsen lehetőségük. Éppen ezért, az érintetti jogok érvényesülésének megerősítése, valamint a bekövetkező adatvédelmi incidensek káros következményei mértékének visszaszorítása érdekében a jogalkotó meghatározott esetekben bejelentési kötelezettséget ír elő az adatkezelőre, nem bízza azt önálló mérlegelésre.[16]

1. A bejelentési kötelezettségről általában

A GDPR által áthatott jogszabályi környezetben – számos intézménnyel egyidejűleg – az adatvédelmi incidensek bejelentési kötelezettségének természete is megváltozott: kivételes, speciális eseti jellegből kikerülve, főszabályi minőségre tett szert. Mindez azt jelenti, hogy a jelenleg hatályos szabályozás értelmében az adatkezelőt – az arra kijelölt személyen, tipikusan az adatvédelmi felelősön keresztül[17] – általános bejelentési kötelezettség terheli az illetékes felügyeleti hatóság irányába adatvédelmi incidens bekövetkezése esetén, s ez alól mentesülni csupán kivételes esetben, az incidens veszélyességi foka alapján van lehetőség. Emiatt az adatkezelőnek a bejelentési kötelezettséget kell automatizmussá tennie; habár gyakorlati oldalról megközelítve a kérdést, mindezt azzal lehet kiegészíteni, hogy nem feltétlenül a bejelentést, hanem legalább az illetékes adatvédelmi hatósággal történő előzetes konzultációt kell megkövetelnie az adatkezelésért felelős jogalanynak.[18]

A jogforrások főszabályát citálva, egyúttal a GDPR és az Infotv. rendelkezéseit egyesítve, az adatkezelő az általa, illetve az adatfeldolgozó által kezelt adatokkal

[15] GDPR (85) preambulumbekezdés; Vö: 2009/136/EK irányelv (61) preambulumbekezdése.
[16] European Union Agency for Fundamental Rights and Council of Europe, 2018, 172.
[17] Baranya, 2016
[18] Calder, 2016, 58.

összefüggésben felmerült adatvédelmi incidenst indokolatlan késedelem nélkül, de legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott,[19] be kell, hogy jelentse az illetékes felügyeleti hatóságnak.[20] E kötelezettség alól azonban van kivétel: amennyiben az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve, nem terheli bejelentési kötelezettség az adatkezelőt.[21]

Szükséges szót ejteni arról a helyzetről is, amikor az adatfeldolgozó[22] eljárása során merül fel az adatvédelmi incidens. Jelen esetkörben a megjelenő többletfaktor, nevezetesen az egyes felek elkülönült alanyi minősége komoly akadályt jelenthet az incidensből eredő következmények megelőzése, illetve a sérelmek mértékének csökkentése szempontjából. Ez az oka annak, hogy a jogforrások konkrét követelményként írják elő azt, hogy az adatfeldolgozó az incidenst az arról való tudomásszerzését követően haladéktalanul, indokolatlan késedelem nélkül jelenti azt az adatkezelőnek,[23] ezzel biztosítva, hogy utóbbi akár objektív határidőként is be tudja tartani a 72 órát. Különös jelentősége van továbbá annak a körülménynek is, hogy az adatfeldolgozó kötelezettsége csupán magára az értesítésre terjed ki, az incidensből eredő kockázat valószínűségének, súlyának felmérésére már nem.[24]

2. A bejelentés tartalma, valamint a szakaszos bejelentés

Annak érdekében, hogy a Hatóság kellően megalapozott ismeretekkel rendelkezzen a bekövetkezett adatvédelmi incidensről, s azzal összefüggésben helytálló intézkedéseket tudjon foganatosítani, elengedhetetlen a lehető legszélesebb körre kiterjedő bejelentés. Ahhoz, hogy az incidensbejelentés ennek az elvárásnak megfeleljen, a jogalkotó mind a regionális, mind pedig a belső jogi jogforrásban rögzítette az annak tartalmára vonatkozó legalapvetőbb követelményeket. A két jogszabály idevágó rendelkezései tartalmilag megegyeznek, azonban az Infotv. 25/J. § (5) bekezdésének magyar terminológiába jobban illeszkedő megfogalmazása miatt ehelyütt annak szabályait veszem át. Ez alapján az adatvédelmi incidens bejelentése akkor tekinthető megfelelőnek, amennyiben abban az adatkezelő

[19] A tudomásszerzés akkor állapítható meg, amikor „az adatkezelő észszerű bizonyossággal meggyőződött arról, hogy olyan biztonsági incidens történt, amelynek következtében a személyes adatok veszélybe kerültek". (WP250, 10.).

[20] GDPR 33. cikk (1) bekezdés és Infotv. 25/J. § (1) bekezdés.

[21] GDPR 33. cikk (1) bekezdés és Infotv. 25/J. § (2) bekezdés.

[22] Terjedelmi okokból az adatfeldolgozóra irányadó részletesebb szabályok bemutatását mellőzöm, azonban az intézmény definiálását szükségesnek tartom. A GDPR 4. cikk 8. pontja alapján adatfeldolgozó „az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel".

[23] GDPR 33. cikk (1) bekezdés, illetve Infotv. 25/J. § (2) bekezdés.

[24] Jóri, 2018, 341.

- „ismerteti az adatvédelmi incidens jellegét, beleértve - ha lehetséges - az érintettek körét és hozzávetőleges számát, valamint az incidenssel érintett adatok körét és hozzávetőleges mennyiségét,
- tájékoztatást nyújt az adatvédelmi tisztviselő vagy a további tájékoztatás nyújtására kijelölt más kapcsolattartó nevéről és elérhetőségi adatairól,
- ismerteti az adatvédelmi incidensből eredő, valószínűsíthető következményeket, és
- ismerteti az adatkezelő által az adatvédelmi incidens kezelésére tett vagy tervezett - az adatvédelmi incidensből eredő esetleges hátrányos következmények mérséklését célzó és egyéb - intézkedéseket."

Ugyanakkor nehezen felderíthető, vagy az érintettek, illetve az adatok széles körét érintő incidens esetén ez nem, vagy csak kivételes erőfeszítés árán teljesíthető a normatívan elvárt 72 órán belül; felmerülhet hát, hogy az alaposságra és teljességre való törekvés kontraproduktívvá válik, és a legnagyobb jóhiszeműség mellett is csak további sérelmet okoz az érintett számára. Olykor az adatvédelmi incidens bekövetkezését követő bárminemű intézkedési késlekedés a személyes adatok biztonsága újabb vagy még súlyosabb sérelmének veszélyét hordozza magában, így például a biztonsági rés befoltozása elsőbbséget kell, hogy élvezzen a sérelem mértékének felderítésével szemben.

Éppen ezért, az egykori 95/46/EK adatvédelmi irányelv 29. cikke szerint létrehozott adatvédelmi munkacsoport egyértelműen rögzítette, hogy „a hangsúlyt nem a pontos számadatok közlésére, hanem az incidens hátrányos hatásainak kezelésére kell fektetni".[25] Ezen túlmenően, a jogforrások egységesen biztosítják annak a lehetőségét, hogy az adatkezelő – a bejelentés utólagos megtételével egyidejűleg – a késedelem igazolására szolgáló indokok előadásával kimentse a mulasztását.[26] Utóbbi szabályt a gyakorlat[27] kiegészítette egy további, a bejelentésre nyitva álló meglehetősen szűk határidő betartását elősegítő megoldással is: „Ha az adatkezelő már észszerű mértékű bizonyossággal bír az incidens bekövetkeztéről, de még nem rendelkezik minden információval azzal kapcsolatban, *érdemes* – a 72 órás határidő betartása érdekében – a szakaszos bejelentés lehetőségével élni. Az ilyen jellegű bejelentések az annak pillanatában nem ismert információkkal később kiegészíthetők, helyesbíthetők, módosíthatók."[28] Ilyenkor tehát az adatkezelő, ha és amennyiben nem tudja valamennyi, a bejelentéshez szükséges információt egyidejűleg közölni, azokat később (de bárminemű indokolatlan késedelem nélkül) részletekben is a Hatóság tudomására hozhatja.

[25] WP250., 15.

[26] GDPR 33. cikk (1) bekezdés, illetve Infotv. 25/J. § (3) bekezdés.

[27] A szabály ma már a hatályos normaanyagnak is része, lásd: GDPR 33. cikk (1) bekezdés, illetve Infotv. 25/J. § (3) bekezdés.

[28] NAIH: Tudnivalók az adatvédelmi incidensek kezeléséről, 2011.

Vagyis az adatvédelmi előírások egy specifikus szabályának, a bejelentési kötelezettségnek való megfelelés érdekében az adatkezelőnek egyáltalán nem szükségszerűen a legrészletesebb, hanem sokszor az adott körülmények között a felderítés, elhárítás és megőrzés háromszögében leghatékonyabbnak minősülő, kompromisszumos megoldást kell választania. Persze, ez a megállapításom csak a mielőbbi bejelentés kapcsán irányadó, az incidenshez kötődő további intézkedések részeként utóbb változatlanul a lehető legteljesebb körben fel kell tárni az eset összes körülményeit.

V. AZ ADATVÉDELMI INCIDENSSEL ÖSSZEFÜGGŐ TOVÁBBI INTÉZKEDÉSEK

Az előbbi szerkezeti egységet záró gondolataimat folytatva, a bejelentési kötelezettség csupán egy – ám annál fontosabb – az adatvédelmi incidensekhez kapcsolódó, (lehetséges) intézkedési jellegű következmények közül. Mindez értelemszerű, amennyiben a távolabbi célokra is fókuszálunk: a felmerült veszélyhelyzet, sérelem nyilvánvalóan nem múlik el, nem kerül felszámolásra és orvoslásra pusztán annál a ténynél fogva, hogy azt az adatkezelő bejelentette az illetékes hatóságnak, illetve az újabb hasonló esetek sem előzhetők meg önmagában ezzel. Mindebből az következik, hogy az adatkezelőt (és adott esetben az adatfeldolgozót) számos további cselekvési-intézkedési kötelezettség terheli, illetve terhelheti az adatvédelmi incidenssel összefüggésben. Ezeknek taxált listája szintén nem állítható fel, hiszen minden helyzet egyedi, s erre csupán az ügy összes körülményének ismerete alapján volna lehetőség; azonban általános jelleggel mégis össze tudok állítani egyfajta cselekvési katalógust.

Elsőként rögzíteni kell azt, hogy az adatvédelmi incidensekkel összefüggő intézkedési folyamat már az incidens felmerülése előtt meg kell, hogy kezdődjön. Ezek elsődlegesen a már érintett adatbiztonsági előírásokkal összhangban álló, megfelelő technikai és szervezési intézkedések megtételét és teljesítését várja el az adatkezelőtől, illetve az adatfeldolgozótól. Az előzetes szervezési intézkedések körébe sorolhatóan meg kell állapodni arról is, hogy a cselekvési kötelezettség hogyan oszlik meg a felek között akkor, amikor az adatvédelmi incidens közös adatkezelés vagy adatfeldolgozó igénybe vétele esetén merül fel.

Az incidens bekövetkeztét követően, ahogyan azt már korábban részleteztem, az adatkezelő főszabály szerint köteles az esetet az adatvédelmi hatóság irányába bejelenteni; a NAIH pedig a jelentésben foglaltak alapján dönt az eljárás lefolytatásáról (ellenőrzés, vizsgálat), illetve indokolt esetben a további szükséges intézkedések meghatározásáról, esetleg szankció kiszabásáról. Ugyanakkor, a joganyag ettől nemcsak enyhébb (bejelentési kötelezettség elmaradása), hanem egyúttal szigorúbb követelményeket meghatározó kivételt is tartalmaz.

A polgári és számos egyéb jogviszonyban[29] is megjelenő együttműködési kötelezettségből eredően, valamint az érintett érdekeinek szem előtt tartását és jogosorvoslati-kártérítési igényének biztosítását szolgálva jelenik meg a GDPR 34. cikkén alapuló, a törvényi főszabálynál szigorúbb adatvédelmi incidenshez fűződő jogkövetkezmény: az érintett tájékoztatása. Ennek értelmében, ha az adatvédelmi incidens valószínűsíthetően legalább magas kockázatúnak minősül, az adatkezelő indokolatlan késedelem nélkül tájékoztatja az érintettet az adatvédelmi incidensről.[30] Ugyanakkor, szükséges ezzel összefüggésben rögzíteni, hogy a hazai jogalkotó az Infotv. szabályozási keretein belül leszűkíti e kötelezettség teljesítésének feltételeit. A magyar szabályrendszer ugyanis az ENISA ajánlásánál valamivel szűkebb körben, csupán abban az esetben minősíti magas kockázatúnak az adatkezelést,[31] illetve az adatvédelmi incidenst, amennyiben az „valószínűsíthetően az érintetteket megillető, valamely alapvető jog érvényesülését lényegesen befolyásolja".[32]

Előfordulhat azonban olyan eset is, hogy ugyan az adatkezelő – az általa megállapított alacsonyabb veszélyességi besorolás következtében – nem értesítette az érintettet a bekövetkezett adatvédelmi incidensről, ám utóbb mégis teljesítenie kell e kötelezettségét. Ez arra a korábban már érintett körülményre vezethető vissza, hogy a Hatóság jogosult a bejelentés, illetve saját vizsgálatainak eredménye alapján felülbírálni az adatkezelő döntését, átminősítve az incidens súlyosságát. Amennyiben e változás következtében az adatvédelmi incidens veszélyessége Magas szintre módosul, úgy az alkalmazandó jogkövetkezmények köre is kibővül. Tehát, amennyiben „az adatkezelő még nem értesítette az érintettet az adatvédelmi incidensről, a felügyeleti hatóság, miután mérlegelte, hogy az adatvédelmi incidens valószínűsíthetően magas kockázattal jár-e, elrendelheti az érintett tájékoztatását".[33]

Az érintett tájékoztatása kötelezettségének elsődleges funkciója tehát egyértelműen az, hogy az érintett lépéseket tudjon tenni az incidens hatásainak elhárítása, jogainak és jogos érdekeinek védelme érdekében.[34] Éppen ezért, a GDPR 34. cikk (2) bekezdése alapján világosan és közérthetően kell az érintettekkel ismertetni az adatvédelmi incidens jellegét, egyúttal pedig közölni kell

- az adatvédelmi tisztviselő vagy egyéb kapcsolattartó nevét és elérhetőségeit;
- az incidensből eredő, valószínűsíthető következményeket; valamint
- az adatkezelő által az incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket is.

[29] Lásd pl.: a munka törvénykönyvéről szóló 2012. évi I. törvény 6. § (2) bekezdés.
[30] GDPR 34. cikk (1) bekezdés.
[31] Infotv. 25/G. § (2) bekezdés.
[32] Infotv. 25/K. § (1) bekezdés.
[33] GDPR 34. cikk (4) bekezdés, illetve kisebb változtatásokkal az Infotv. 25/K. § (4) bekezdése is.
[34] Information Comissioner's Office, 2018, 188.

Ugyanakkor, bizonyos keretek között mégis mentesülhet az adatkezelő a fentiekben kifejtett értesítési kötelezettség alól. Így nem kell értesíteni az érintettet az incidensről, ha megfelelő előzetes vagy utólagos műszaki és szervezési védelmi intézkedések következtében valószínűsíthetően nem áll fenn a sérelem veszélye; illetve akkor sem, ha az érintett közvetlen tájékoztatása aránytalan erőfeszítéssel lenne csak teljesíthető, vagy azt törvény egyenesen kizárja.[35]

Szintén elvárás az adatkezelővel szemben, hogy az elszámoltathatóság elvével[36] összhangban a bekövetkezett adatvédelmi incidensekről – mind az incidens természetétől, mind pedig annak súlyától függetlenül – részletes nyilvántartást vezessen. Ennek részeként (élve a GDPR által biztosított eltérési lehetőséggel, a regionális jogforrás előírásainál[37] lényegesen részletesebb belsőjogi szabályok alapján) az adatkezelő az egyes adatkezelési műveleteiről, az adatvédelmi incidensekről és az érintett hozzáférési jogával kapcsolatos intézkedésekről nyilvántartást vezet, melyben rögzíti a következőket:

- az adatkezelő(k), valamint az adatvédelmi tisztviselő nevét és elérhetőségeit,
- az adatkezelés célját vagy céljait,
- személyes adatok (tervezett) továbbítása esetén az adattovábbítás címzettjeinek körét,
- az érintettek, valamint a kezelt adatok körét,
- profilalkotás alkalmazása esetén annak tényét,
- nemzetközi adattovábbítás esetén a továbbított adatok körét,
- az adatkezelési műveletek – ideértve az adattovábbítást is – jogalapjait,
- ha az ismert, a kezelt személyes adatok törlésének időpontját,
- a végrehajtott műszaki és szervezési biztonsági intézkedések általános leírását,
- az általa kezelt adatokkal összefüggésben felmerült adatvédelmi incidensek bekövetkezésének körülményeit, azok hatásait és a kezelésükre tett intézkedéseket,
- az érintett hozzáférési jogának érvényesítését korlátozó vagy megtagadó intézkedésének jogi és ténybeli indokait.[38]

A fentiekből látható, hogy a nyilvántartási kötelezettség, a korábbiakban kifejtett bejelentési-értesítési kötelezettséggel együtt, mintegy „passzív következménye" az adatvédelmi incidensnek, azaz nem közvetlenül annak elhárításához, a sérelem mértékének csökkentéséhez, illetve a további incidensek bekövetkezésének visszaszorításához, hanem sokkal inkább az adatkezelő ellenőrizhetőségéhez és elszámoltathatóságához, valamint – közvetett módon – a további

[35] GDPR 34. cikk (3) bekezdés, illetve Infotv. 25/K. § (2) bekezdés.

[36] GDPR 5. cikk (2) bekezdés: Az adatkezelő felelős az 5. cikk (1) bekezdésében meghatározott alapelveknek való megfelelésért, továbbá képesnek kell lennie e megfelelés igazolására.

[37] Ld. GDPR 33. cikk (5) bekezdés.

[38] Infotv. a 25/E. § (1) bekezdés.

incidensek esetleges megelőzéséhez szükséges. Ezzel szemben természetesen vannak még az előbbi célokat közvetlenül szolgáló, ezáltal általam csak „aktív következményeknek" nevezett konzekvenciái is.

E kötelezettségek az adatbiztonság már korábban kifejtett követelményeire vezethetők vissza. Az adatvédelmi incidensek egy vagylagos körülményt ugyanis szükségszerűen feltételeznek: az adatkezelő vagy nem tett meg mindent annak érdekében, hogy az adatbiztonsági elvárásoknak megfeleljen, vagy pedig a mindezek ellenére bekövetkezett adatvédelmi incidens hatására a sérült biztonsági rendszerek helyreállítása, illetve a biztonsági intézkedések felülvizsgálata szükséges, hiszen meg kell előzni az újabb incidensek bekövetkezését. Bármelyik helyzet is álljon fenn, közös mindkettőben, hogy aktív, tevőleges cselekvést igényel az adatkezelő (illetve az adatfeldolgozó) részéről. Ezek az intézkedések – igazodva a bekövetkezett incidens természetéhez, jellegéhez – nyilvánvalóan rendkívül sokfélék lehetnek, így csupán példálózó jelleggel ide sorolhatók a következők:

- új biztonsági protokollok (például kétlépcsős azonosítás) bevezetése;
- az adatkezelési szabályzat felülvizsgálata, szigorúbb rendelkezések rögzítése;
- új adatvédelmi tisztségviselő kijelölése, adott esetben külső szolgáltató segítségének igénybe vétele;
- a belső hálózathoz csatlakozó eszközök és külső hálózati elérések (például VPN-kliensek használatának) korlátozása;
- a külső szoftverek és eszközök használatának tilalma.

IRODALOM

- A 29. cikk szerinti adatvédelmi munkacsoport: Iránymutatás az adatvédelmi incidensek (EU) 2016/679 rendelet szerinti bejelentéséről (18/HU, WP250rev.01).
- A Nemzeti Adatvédelmi és Információszabadság Hatóság Beszámolója a 2018. évi tevékenységéről. (Elérhető: https://naih.hu/eves-beszamolok?download=24:naih-beszamolo-a-2018-evi-tevekenysegrol. Letöltés ideje: 2022. október 12.).
- Árvay Viktor (2018): Adatbiztonság. In: Péterfalvi Attila – Révész Balázs – Buzás Péter: *Magyarázat a GDPR-ról.* Wolters Kluwer, Budapest.
- Baranya Zsolt (2016): A belső adatvédelmi felelős és az elektronikus információs rendszerek biztonságáért felelős személy feladatainak összehasonlítása és a feladatok ellátásának összefüggései. In: *Infokommunikáció és Jog.* 2016/2-3. sz.
- Buday-Sántha Andrea (2019): „Minek nevezzelek?" Az információs jogok jelene és jövőbeli szabályozási kihívásai. In: *JURA.* 2019/1. sz.
- Calder, Alan (2016): *EU GDPR – A Pocket Guide.* IT Governance Publishing, Ely.
- European Union Agency for Fundamental Rights and Council of Europe (2018): *Handbook on European data protection law 2018 edition.* Publications Office of the European Union, Luxemburg.
- Győrffyné Holló Krisztina (2021): Információbiztonság, avagy incidens kontra biztonságtudatos viselkedés. *Infokommunikáció és Jog.* 2021/1. sz.

- Information Comissioner's Office (2018): *Guide to the General Data Protection Regulation (GDPR).* ICO, Wilmslow.
- Jóri András (2018): Az adatvédelmi incidensek és kezelésük. In: Jóri András (szerk.): *A GDPR magyarázata.* HVG-ORAC Lap- és Könyvkiadó, Budapest.
- Manso, Clara Galan – Górniak, Sławomir (2013): *Recommendations for a methodology of the assessment of severity of personal data breaches.* ENISA. (Elérhető: https://www.enisa.europa.eu/publications/dbn-severity/at_download/fullReport. Letöltés ideje: 2021. március 4.).
- Mayer Erika – Verebics János (2002): Információbiztonság, információs rendszerek biztonsága, információs jogbiztonság. *Gazdaság és Jog.* 2002/11. sz.
- NAIH/2019/2471/6.
- NAIH: Tudnivalók az adatvédelmi incidensek kezeléséről. (Elérhető: https://www.naih.hu/tudnivalok-az-adatvedelmi-incidensek-kezeleserol. Letöltés ideje: 2021. március 6.).
- NAIH-1881-5/2013/H.

JOGFORRÁSOK

- A munka törvénykönyvéről szóló 2012. évi I. törvény.
- Az Európai Parlament és a Tanács (EU) 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 rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet).
- Az Európai Parlament és a Tanács az Európai Hálózat- és Információbiztonsági Ügynökség létrehozásáról szóló 460/2004/EK rendelete (2004. március 10.).
- Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény.