Az adatvédelmi incidens

Árvay Viktor György

NEMZETI KÖZSZOLGÁLATI EGYETEM
BUDAPEST

Szerző:
© Dr. Árvay Viktor György

Szakmai lektor:
Dr. Péterfalvi Attila

Olvasószerkesztő:
Császár-Biró Anna

A kézirat lezárásának dátuma:
2019. október 02.

Kiadás éve:
2019

TARTALOM

1. ELŐSZÓ

1.1. Adatvédelmi incidensek helye az adatvédelemben

Az Európai Parlament és a Tanács (EU) által elfogadott, 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 2016/679 Rendelet (a továbbiakban: GDPR) nagyobb hangsúlyt fektet az adatbiztonság területére. Ez egyrészről megjelenik abban, hogy részletesebb, pontosabb szabályokat tartalmaz ezen a területen, másrészről olyan új intézményeket, kötelezettségeket vezet be, amelyek elősegítik az adatbiztonsághoz történő tudatosabb hozzáállást. Ez utóbbira példa az adatvédelmi incidensek bejelentésének, kezelésének a kötelezettsége. A jogalkotó az információbiztonság területén régóta ismert jó gyakorlatot illesztett bele az adatvédelmi rezsimbe. Ennek megfelelően az adatvédelmi incidensek azonosítása és kezelése támaszkodhat az információbiztonsági incidensek azonosításának és kezelésének gyakorlati tapasztalataira.

Az adatvédelmi incidensek kezelésének a középpontjában az érintettek jogainak és szabadságainak, a magánszférájuknak és a személyes adataiknak a védelme áll. Ennek megfelelően az adatvédelmi incidensekhez kapcsolódó adatkezelői, adatfeldolgozói kötelezettségekre egy compliance (megfelelőség) eszközként, illetve egy elszámoltathatósági mechanizmusként érdemes tekinteni.

Az adatvédelmi incidensekhez kapcsolódó adatkezelői, adatfeldolgozói kötelezettségek a korábban már említett alapelvek közül az elszámoltathatóság elvéhez, illetve az integritás és bizalmas jelleg elvéhez szorosan kapcsolódnak. Emellett megjeleníti a GDPR-ban érvényre jutatott kockázatalapú megközelítést is.[1]

Az elszámoltathatóság elve alapján az adatkezelő felelős a személyes adatok kezelésére vonatkozó alapelveknek történő megfelelésért, továbbá képesnek kell lennie e megfelelés igazolására.[2] Az adatkezelő az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre annak biztosítása és bizonyítása céljából, hogy a személyes adatok kezelése a GDPR-ral összhangban történik. Ezeket az intézkedéseket az adatkezelő felülvizsgálja és szükség esetén naprakésszé teszi.[3]

Az elszámoltathatóság nem új jelenség sem a vállalati kultúrában, sem az adatvédelemben. A nagyvállalati környezetben jól ismert compiance-hez hasonló intézményről beszélhetünk. Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) 22. §-a pedig korábban is tartalmazott az elszámoltathatósághoz hasonló kötelezettséget, bár ez csak a bírósági jogérvényesítéshez volt köthető. Ennek megfelelően nem a jogintézmény megjelenése, hanem annak alapelvi szintre emelése a GDPR egyik leghangsúlyosabb újítása. Az adatkezelőknek ezentúl sokkal nagyobb tudatossággal kell az adatkezeléseiket végezni. Az adatkezelés megtervezésétől kezdve az adatkezelés megkezdésén át egészen a kezelt személyes adatok törléséig valamennyi adatkezelési műveletet úgy kell megvalósítaniuk, hogy bármelyik pillanatban bizonyítani tudják, hogyan feleltek meg az adatvédelmi előírásoknak.

---

1 Péterfalvi – Révész – Buzás (szerk.): Magyarázat a GDPR-ról. Wolters Kluwer, Budapest, 2018., 213.

2 GDPR 5. cikk (2) bekezdés.

3 GDPR 24 cikk (1) bekezdés.

Az elszámoltathatóság elve mindenek felett álló alapelvvé vált az adatvédelemben. Ehhez az alapelvhez a GDPR valamennyi rendelkezését hozzá lehet kapcsolni, és ezt az alapelvet az adatkezelőknek mindig szem előtt kell tartaniuk. Az elszámoltathatóság elve lényegében azt jelenti, hogy az adatkezelőknek a szervezeti kultúrájukat, továbbá valamennyi tevékenységüket az adatvédelemi megfontolásokra tekintettel kell kialakítaniuk, végezniük. Az adatkezelőknek minden egyes lépésüknél el kell gondolkodniuk, hogy az adatvédelmi előírásokat miként vették figyelembe.

Természetesen ezen az általános attitűdön túl a GDPR számos elvi és gyakorlati eszközzel is megpróbálja segíteni az elszámoltathatóság elvének érvényesülését. Ennek megfelelően az elszámoltathatóság követelményének teljesítését segíti elő többek között az adatvédelmi incidensekkel kapcsolatos szabályozás is.[4]

Az adatkezelőnek törekednie kell arra, hogy olyan szervezeti és technikai intézkedéseket tegyen, amelyekkel megelőzi az adatvédelmi incidenseket, továbbá olyanokat, amelyek az adatvédelmi incidensek sikeres kezeléséhez hozzájárulnak, illetve csökkentik az esetleges adatvédelmi incidenseknek az érintettek jogaira és szabadságaira gyakorolt hatását.

Az integritás és bizalmas jelleg elve alapján 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.[5]

A kockázatalapú megközelítéssel a GDPR egy adatvédelmi incidens kezelésénél azt várja el az adatkezelőtől, hogy megtegye a megfelelő technikai és szervezési intézkedéseket, amelyeket az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével, és ennek során az adatkezelőnek a tudomány és technológia állására, a végrehajtás kockázatára és a védelmet igénylő személyes adatok jellegével összefüggő költségekre is figyelemmel kell lennie.[6]

A fenti alapelveket és általános kötelezettségeket azért szükséges említeni, mert az adatvédelmi incidensekkel kapcsolatos kötelezettségek nem merülnek ki pusztán a nyilvántartás vezetésében, a hatóság felé történő bejelentésben vagy az érintett irányába történő kommunikációban. Az elszámoltathatóság alapelvéből adódóan ez alatt jóval szélesebb körű kötelezettséget értünk, hiszen magában foglalja az adatvédelmi incidensek megelőzésére tett lépéseket, valamint bele kell érteni az előbb említett kötelezettségek teljesítésére történő felkészülést is. A kockázatalapú megközelítés pedig ezeket a kötelezettségeket helyezi az észszerűség keretei közé, hiszen köztudott, hogy tökéletes biztonság nem létezik és további erőforrások bevonásával a biztonság fokozata mindig tovább növelhető, ezért az elvárható biztonság mértékét a GDPR az adatkezelés jellegére, a kockázatok valószínűségére és súlyosságára, illetve a megvalósítási költségekre is tekintettel követeli meg.

1.2. Az adatvédelmi incidensek korábbi szabályozása

A legelső adatvédelmi jogszabályunk a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény (a továbbiakban: Avtv.) nem tartalmazott konkrét szabályozást az adatvédelmi incidensekre vagy azok kezelésére. Az az általános adatbiztonsági előírások érvényesülése során volt levezethető. Az adatvédelmi incidensek kivizsgálása már az adatvédelmi biztos gyakorlatában is megjelent, de akkor még konkrét szabályozás hiánya miatt az Avtv. 10.§-ban meghatározott adatbiztonsági követelmények ellenőrzéseként. Az adatvédelmi biztos ilyen követelmények megsértéseként értékelte, amikor egy cég előfizetői adatbázisát tartalmazó CD

[4] A Nemzeti Adatvédelmi és Információszabadság Hatóság beszámolója a 2016. évi tevékenységéről.
[5] GDPR 5. cikk (1) bekezdés f) pont.
[6] GDPR 32. cikk.

illetéktelenek számára hozzáférhetővé vált. Ugyanígy hasonló jogsértést állapított meg, amikor nagy mennyiségben találtak személyes adatokat is tartalmazó iratokat egy MÉH-telepen.[7]

Az Avtv.-t váltó adatvédelmi szabályozás az Infotv. eleinte ugyancsak nem tartalmazott konkrét szabályokat, fogalmakat az adatvédelmi incidensekre vonatkozóan. Az adatvédelmi incidensek értékelése továbbra is az adatbiztonságról szóló előírások részeként került vizsgálatra. Így például akkor, amikor a Hatóság bírságot szabott ki az Infotv. 5-7. §-ban meghatározott adatbiztonsági követelmények megsértése miatt abban az esetben, amikor nyitott, nyílászáró nélküli istállóban, felszámolt szervezetek, köztük egykori állami vállalatok, szövetkezetek személyes adatokat tartalmazó iratanyagát tárolták őrizetlenül,[8] vagy amikor bírságot szabtak ki egy gyenge biztonsági beállításokat tartalmazó és meg is támadott honlap üzemeltetésért.[9]

2015. október 1-jén az Infotv. módosítása azonban bevezette a magyar adatvédelmi szabályozásba az adatvédelmi incidens fogalmát. Ennek értelmében adatvédelmi incidens volt az adatbiztonság olyan sérelme, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisülését, elvesztését, módosulását, jogosulatlan továbbítását vagy nyilvánosságra hozatalát, vagy az azokhoz való jogosulatlan hozzáférést eredményezte (Infotv. 3. § 26. pont). A módosítás egyben kötelezte az adatkezelőket az incidensek nyilvántartására, amely értelmében az adatkezelő – ha belső adatvédelmi felelőssel rendelkezik, a belső adatvédelmi felelős útján – az adatvédelmi incidenssel kapcsolatos intézkedések ellenőrzése, valamint az érintett tájékoztatása céljából nyilvántartást kellett, hogy vezessen, amely tartalmazza az érintett személyes adatok körét, az adatvédelmi incidenssel érintettek körét és számát, az adatvédelmi incidens időpontját, körülményeit, hatásait és az elhárítására megtett intézkedéseket, valamint – ha volt ilyen – az adatkezelést előíró jogszabályban meghatározott egyéb adatokat [Infotv. 15. § (1a)].

Fontos azonban kiemelni, hogy az Infotv. módosítását követő szabályozásból is levezethető volt az adatvédelmi incidensek kezelésére vonatkozó adatkezelői kötelezettség, hiszen az adatvédelmi incidensek nyilvántartásának a részét képezte az adatvédelmi incidensek hatásainak a felmérésére, illetve az adatvédelmi incidensek elhárítására tett intézkedések nyilvántartása. Ebből következően a jogalkotó ugyan az incidensek NAIH számára történő bejelentését nem írta elő adatkezelői kötelezettségként, de minden más később a GDPR-ból levezethető adatkezelői kötelezettség közvetett módon következett a normaszövegből.

A GDPR alkalmazandóvá válását megelőző incidensszabályozás jó példája a NAIH/2018/356/3/H számú hatósági eljárás. A kérdéses ügyben a Hatóság indított vizsgálatot, miután bejelentések érkeztek arról, hogy egy új online jegyértékesítési rendszerből könnyen kinyerhetők az ott regisztrálók személyes adatai, melyhez illetéktelen személyek hozzá is fértek. A kinyert adatbázis a sajtóhoz is eljutott, akik továbbították azt a Hatóság felé. Az eljárás alatt a Hatóság megállapította, hogy sor került az adatbiztonság olyan sérülésére, amely a kezelt adatokhoz való jogosulatlan hozzáférést eredményezte, vagyis az Infotv. 3. § 26. pontja szerinti adatvédelmi incidens történt. Az adatkezelő ugyanakkor kezdetben nem tekintette incidensnek az esetet, majd a Hatóság eljárása alatt – másfél hónappal az incidens megtörténte után – már incidensnek minősítette, de az incidens feltárására kapcsán nem tudott konkrét intézkedésről beszámolni. A határozat kimondta, hogy az adatbiztonsággal kapcsolatos tervezés és a szükséges intézkedések felismerésének hiányát támasztja alá, hogy az adatkezelő által tett egyetlen konkrét intézkedés az online rendszer leállítása volt. Az adatkezelő tehát nem tett meg mindent az adatvédelmi incidens körülményeinek, súlyosságának, valamint az érintettekre gyakorolt hatásának kivizsgálása érdekében, továbbá nem csak az incidens előtt, de azt követően sem tette meg a szükséges adatbiztonsági intézkedéseket.

A szabályozás ekkor még csak nyilvántartási kötelezettséget írt elő az adatkezelők részére, azonban az incidens kezelés belső szabályozással történő meghatározásának (szervezési intézkedés),

---

7 Jóri – Soós: Adatvédelmi jog. HVG-ORAC, Budapest, 2016. 214-214.

8 NAIH-2087-5/2012/H.

9 NAIH-559-26/2013/H.

az adatbiztonság megfelelő szintje biztosításának (technikai intézkedés), valamint magas kockázat esetén az érintettek értesítésének követelménye az Infotv. szakaszaiból már ekkor levezethető volt.

Részben korábbi szabályozásnak vagy helyesebben párhuzamos szabályozásnak tekinthetőek azok az uniós szabályozáson nyugvó normák, amelyek egy-egy területen külön adatvédelmi incidensbejelentési kötelezettségeket írtak elő az adatkezelő számára.

Hasonló jogintézmény párhuzamosan az elektronikus hírközlésről szóló 2003. évi C. törvény (a továbbiakban: Eht.) alapján is létezett az elektronikus hírközlés szolgáltatók számára, amely az Elektronikus hírközlési adatvédelmi irányelv átültetése révén jelent meg a magyar jogrendszerben. A „személyes adatok megsértésének" bejelentési kötelezettsége[10] az Eht. 156.§ (3) bekezdése és a 4/2012. (I. 24.) NMHH rendelet 5. §-ban foglaltak szerint a mai napig fennáll. Ennek megfelelően, amennyiben előfizetői személyes adatok „véletlen, vagy jogellenes kezelése vagy feldolgozása, így különösen megsemmisítése, elvesztése, módosítása, jogosulatlan felfedése, nyilvánosságra hozatala, vagy az azokhoz való jogosulatlan hozzáférés" esete áll fenn, a szolgáltató haladéktalanul, de legkésőbb 24 órán belül köteles a Nemzeti Média és Hírközlési Hatóságnak azt jelenteni. A GDPR 95. cikke értelmében ez a kötelezettség továbbra is fennáll, és az NMHH felé jelentett Eht. szabályai alapján jelentett incidenst a NAIH számára már nem kell bejelenteni. Fontos azonban kiemelni, hogy ez nem minden az elektronikus hírközlési szolgáltatóknál bekövetkező incidensre vonatkozik. Ha az incidens nem az előfizetői személyes adatokat, hanem más, például a munkavállalók, személyes adatokat érintenek, akkor azt a GDPR. alapján a NAIH számára kell bejelenteni.

Egy másik bejelentési kötelezettséget rögzít az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény és az információs társadalommal összefüggő szolgáltatások elektronikus információbiztonságának felügyeletéről és a biztonsági eseményekkel kapcsolatos eljárásrendről szóló 270/2018. (XII. 20.) Korm. rendelet által implementált úgynevezett NIS irányelv, amely az online piactér, online keresőszolgáltatás, felhőalapú számítástechnikai szolgáltatás esetén előírja a digitális szolgáltatást nyújtó vállalkozások jelentős biztonsági eseményekkel kapcsolatos bejelentési kötelezettségét a Nemzetbiztonsági Szakszolgálat felé. Fontos kiemelni, ha a biztonsági esemény személyes adatokat is érint, akkor azt a NAIH felé is jelenteni kell.

Végül pedig a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról szóló 910/2014/EU rendelet, vagyis az eIDAS-rendelet 19. cikk (2) bekezdése alapján az úgynevezett bizalmi szolgáltatók értesítik a felügyeleti szervet – Magyarországon a Nemzeti Média és Hírközlési Hatóságot – a biztonság megsértéséről vagy az adatok sértetlenségének megszűnéséről, amennyiben az jelentős hatást gyakorol a bizalmi szolgáltatásra vagy az annak keretében tárolt személyes adatokra. Ha az incidens személyes adatokat is érint, akkor azt a NAIH felé is jelenteni kell.

[10] Továbbá az adatvédelmi incidens nyilvántartási és az eset körülményeitől függően az ügyfelek tájékoztatási kötelezettsége.

2. BEVEZETÉS

2.1. Az adatvédelmi incidens fogalma

Az adatkezelőnek ahhoz, hogy a GDPR-ban konkrétan megfogalmazott, az adatvédelmi incidensekhez kapcsolódó kötelezettségeket teljesíteni tudja, először az adatvédelmi incidenseket szükséges azonosítania. Ehhez elengedhetetlen feltétel az adatvédelmi incidensek GDPR-ban rögzített fogalmának részletes ismerete.

Adatvédelmi incidens 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.[11]

Az említett fogalmi elemek jól ismert információbiztonsági megjelöléseket jelölnek. A személyes adat megsemmisítése azt jelenti, hogy a személyes adat már nem létezik, legalábbis nincs meg olyan formátumban, amelyben az adatkezelő számára bármilyen módon felhasználható lenne. A személyes adatok elvesztéséről akkor beszélhetünk, ha a személyes adat továbbra is létezik, de az adatkezelő nem fér hozzá, nincs a birtokában. A személyes adatok megváltoztatásáról akkor beszélhetünk, ha a személyes adat állapotában, tartalmában, illetve megjelenésében módosulás történik. Jogosulatlan közlés akkor következik be, ha arra illetéktelen személyekkel a személyes adatot megosztják, míg jogosulatlan hozzáférésről akkor beszélhetünk, ha illetéktelen személy képes a személyes adatot megismerni. A személyes adatok károsodásáról pedig akkor beszélhetünk, ha az eredeti adatállományt megváltoztatták, az nem teljes.

Az adatvédelmi incidensek során ezeknek a fogalmaknak az ismerete és elhatárolása jelentőséggel bír, hiszen az incidensek vizsgálatában, kockázati besorolásában szerepet játszanak.[12]

A fent említett fogalom két fontos eleme, hogy személyes adatot kell érintenie az adatvédelmi incidensnek, illetve az adatvédelmi incidensnek a biztonság sérüléséből kell adódnia.

Ha a biztonság sérülése révén nem személyes adatot érint az incidens, hanem például egy know-howhoz vagy egy személyes adatokat nem tartalmazó üzleti titokhoz jogosulatlanul férnek hozzá. Például, ha egy szoftver értékesítő cég szerveréhez férnek hozzá jogosulatlanul, és onnan licenszkódokat tartalmazó adatbázist másolnak ki, akkor nem beszélhetünk adatvédelmi incidensről, hiszen a biztonság ugyan sérült, de személyes adatokat nem érintett az incidens. Tehát nem minden biztonsági incidens adatvédelmi incidens, de minden adatvédelmi incidens biztonsági incidens.

További fontos eleme a fogalomnak, hogy a biztonság sérüléséből kell következnie az incidensnek, így nem adatvédelmi incidens, ha az adatkezelő normál működése során, a kialakított és követett eljárásrend vezet az incidenshez. Nem beszélhetünk adatvédelmi incidensről például, ha a rosszul megtervezett regisztrációs felületen az érintett helyett az adatkezelő előre bepipálja, hogy az érintett hozzájárul bizonyos személyes adatainak egy meghatározott direkt-marketing üzeneteket küldő vállalkozáshoz történő továbbításához. Ebben az esetben az érintett személyes adatainak a jogosulatlan közlése nem a biztonság sérüléséből adódik, ezért nem adatvédelmi incidensről, hanem jogellenes adatkezelésről van szó. Ugyancsak nem beszélhetünk a biztonság sérüléséről, ha valaki az illegális szemetelőket úgy akarja megleckéztetni, hogy fotókat készít róluk, és azokat nyilvánosan

---

[11] GDPR 4. cikk 12. pont.

[12] Péterfalvi et. al. 2018., 215.

közzéteszi, hiszen ilyenkor nem a biztonság sérüléséből adódik a jogellenes adatkezelés, hanem az adatok nyilvánosságra hozatala az adatkezelő célja és szándéka volt. Ebben az esetben is jogellenes adatkezelésről van szó, de az nem érinti a GDPR 33. és 34. cikkét. Tehát nem minden adatvédelmi jogsértés adatvédelmi incidens, de minden adatvédelmi incidens adatvédelmi jogsértés.

A biztonság fogalmára vonatkozóan általánosan elfogadott meghatározást nem találni. Elfogadhatjuk azt a megközelítést, miszerint a biztonság az az állapot, amelynél a védelmi intézkedések a fenyegetések általi károkozás kockázatát elviselhető szintűre csökkentik. Az adatvédelmi jogban irányadó értelmezés szerint a biztonság alatt egyfelől az adatbiztonságot értjük.

Az adatkezelő a tudomány és technológia állása, a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja, ideértve adott esetben, többek között:

- a személyes adatok álnevesítését és titkosítását;
- a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítását, integritását, rendelkezésre állását és ellenálló képességét;
- fizikai vagy műszaki incidens esetén az arra való képességet, hogy a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását kellő időben vissza lehet állítani;
- az adatkezelés biztonságának garantálására hozott technikai és szervezési intézkedések hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárást.

A biztonság megfelelő szintjének meghatározásakor kifejezetten figyelembe kell venni az adatkezelésből eredő olyan kockázatokat, amelyek különösen a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítéséből, elvesztéséből, megváltoztatásából, jogosulatlan nyilvánosságra hozatalából vagy az azokhoz való jogosulatlan hozzáférésből erednek.[13]

Így az adatkezelőnek megfelelő technikai és szervezési intézkedések alkalmazásával kell végezni az adatkezelést. Ezen intézkedéseket az adatkezelőnek az adatkezelés jellegére, körülményeire, az érintettek jogaira jelentett kockázatokra figyelemmel kell végrehajtania, amelyek során tekintettel lehet a technológia fejlettségére és a megvalósítás költségeire. A megfelelő technikai-szervezési intézkedés célja, hogy az adatkezelő – illetve az adatfeldolgozó – megelőzze az adatvédelmi incidensek bekövetkezését, amennyiben a megvalósított intézkedések nem bizonyulnak kellően hatékonynak, akkor emiatt az adatbiztonság sérül, és adatvédelmi incidens valósulhat meg. Ugyancsak sérül a biztonság, ha az adatvédelmi incidens annak a következménye, hogy a megfelelő technikai és szervezési intézkedéseket nem tartották be. A biztonság sérülése az is, amikor az adatkezelő – illetve az adatfeldolgozó – nem hozza meg az adatkezeléssel arányos és elvárható adatbiztonsági intézkedéseket, amelynek elmulasztása adatvédelmi incidenshez vezet. Ebben az esetben a biztonság sérülése elvi szinten jelentkezik, mivel az adatkezelő nem tett megfelelő biztonsági intézkedéseket, de ennek elvárhatóságából fakadóan mégis olyannak kell a mulasztást tekinteni, mint amely a biztonság sérülését eredményezte.

A biztonság átmeneti sérülése adatvédelmi incidensnek számíthat, különösen, ha az adatokhoz való hozzáférés hiánya jelentős kihatással lehet az érintettek személyek jogaira és szabadságaira. A bejelentés szükségességét a kockázat megléte, vagy annak hiánya határozza meg.[14] Így például mindenképpen incidensnek számít, ha egy zsarolóvírus letitkosítja egy magán plasztikai sebészet pácienseinek egészségügyi adatait tartalmazó kartonjait, és ezért kezelések maradnak el. Még akkor is, ha az adatkezelő egy-két napon belül biztonsági mentésből az adatokat helyreállítja.

---

13 GDPR 32. cikk.

14 A 29. cikk szerinti munkacsoport iránymutatása az adatvédelmi incidensek (EU) 2016/679 rendelet szerinti bejelentéséről (a továbbiakban: WP250).

Ugyanakkor a biztonság sérülésének hiányában nem minősül adatvédelmi incidensnek, ha a visszaélésre használt adatok nem az adatkezelőtől kerültek ki. Erre példa, ha az érintettől valamilyen módon a támadók kicsalják egy online szolgáltatáshoz használt azonosító adatait és jelszavát. Majd oda belépve visszaélnek az érintett személyes adataival. Ebben az esetben az adatkezelőnél nem lépett fel a biztonság sérülése, így a visszaéléssel kapcsolatosan nem is tehető felelőssé, nem terhelik a GDPR 33. és 34. cikkében leírt kötelezettségek.

Az adatvédelmi incidens fogalmának nem szükséges eleme sem a rosszhiszeműség, sem a jogellenes magatartás. Továbbá az incidenst nem csak az adatkezelő magatartása idézheti elő, hanem akár harmadik személy is, bár az esetek döntő többségében az adatkezelő valamilyen szintű gondatlansága megállapítható. Ugyanúgy adatvédelmi incidensnek minősül, ha az adatkezelő alkalmazottja véletlenül törli a személyes adatot, vagy ha egy nem megfelelően frissített szoftver hibájából adódóan törlődik, vagy egy ismert, de nem javított sérülékenységet kihasználva külső támadó törli azt.

Az információbiztonságban jól ismert fogalmakat használva az adatvédelmi incidenseket alapvetően három kategóriába sorolhatjuk. Egyrészről létezhet bizalmassági incidens, amely a személyes adatok véletlen vagy felhatalmazás nélküli közlését, illetve az ezekhez való hozzáférést jelenti. Másrészről sértetlenséggel kapcsolatos incidens, amely a személyes adatok véletlen vagy jogtalan megváltoztatását foglalja magába. Harmadrészről megkülönböztethetünk hozzáférhetőséggel kapcsolatos incidens, amely a személyes adatok véletlen vagy jogtalan megsemmisítését vagy ezek elvesztését eredményezi. A körülményektől függően egy adatvédelmi incidens több kategóriába is besorolható, például egy zsarolóvírus, amely a személyes adatokat nem csak titkosítja, hanem le is másolja és elküldi egy távoli szerverre egyszerre bizalmassági és hozzáférhetőséggel kapcsolatos incidens.

3. AZ ADATVÉDELMI INCIDENS KOCKÁZATAINAK ELEMZÉSE

3.1. Az adatvédelmi incidens kockázati besorolásáról általában

A GDPR 33. és 34. cikke egzakt módon, külön nevesítve három adatkezelői kötelezettséget ír elő. Egyrészről az adatkezelő nyilvántartja az adatvédelmi incidenseket, feltüntetve az adatvédelmi incidenshez kapcsolódó tényeket, annak hatásait és az orvoslására tett intézkedéseket.[15] Másodsorban az adatvédelmi incidenst az adatkezelő indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, bejelenti a felügyeleti hatóságnak, kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve.[16] Harmadrészről, 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.[17]

A fentiekből következik, hogy az adatkezelőnek először az adatvédelmi incidens kockázati besorolását kell elvégeznie, hogy ennek megfelelően azonosíthassa, mely kötelezettségeknek kell eleget tennie. Emellett, mint fentebb láthattuk, a biztonságnak is fontos fogalmi eleme az elviselhető szintű kockázat. A kockázat meghatározása tekintetében sincs egységesen alkalmazott fogalom, azonban elfogadhatjuk azt a definíciót, miszerint olyan eshetőség, amely súlyosság és valószínűség szempontjából jellemez valamilyen eseményt és annak következményeit. Az adatkezelő jellemzően az adatkezelés megkezdését megelőzően felméri az érintett természetes személyek jogaira és szabadságaira vonatkozó előzetes kockázatot a bizalmasság, sértetlenség, rendelkezésre állás szempontjából, figyelembe véve a kockázat valószínűségét és súlyosságát. A kockázatértékelés eredménye alapján tudja majd az adatkezelő megválasztani az adatkezeléshez kapcsolódó adatbiztonsági intézkedéseket, adatvédelmi incidens esetén pedig kezelni az incidens hatásait, teljesíteni az incidensbejelentésre, érintettek tájékoztatására vonatkozó kötelezettségét.

Az adatvédelmi incidens azonosítását követően az adatkezelő következő feladata azt eldönteni, hogy az adott incidens milyen kockázatot jelent az érintett természetes személyek jogaira és szabadságaira nézve. Ez több szempontból fontos, egyrészről az adatkezelő a kockázat valószínűségéhez és súlyosságához mérten tudja kezelni az incidens hatásait; másrészről meg tudja állapítani, hogy bejelentési, illetve tájékoztatási kötelezettsége keletkezett-e.

A kockázatelemzést rögtön az incidensről történő tudomásszerzést követően megkezdi az adatkezelő, és ezt egészen az incidens kezelés lezárásáig folyamatosan naprakészen tartja. Tehát ez a tevékenységet a többi kötelezettség mellett párhuzamosan, folyamatosan végzi az adatkezelő.

A kockázat olyan eshetőség, amely a súlyosság és valószínűség szempontjából jellemez valamilyen eseményt és annak következményeit. Az incidenskezelés során az érintettek jogaira és szabadságaira veszélyt jelentő kockázatot szükséges vizsgálnunk. Ez az utalás elsősorban az adatvédelemhez és a magánélet tiszteletben tartásához való jogra vonatkozik, de érinthet más alapvető jogot is, így a

---

15 GDPR 33. cikk (5) bekezdés.
16 GDPR 33. cikk (1) bekezdés.
17 GDPR 34. cikk (1) bekezdés.

szólásszabadságot, a gondolatszabadságot, a mozgás szabadságát, a hátrányos megkülönböztetés tilalmát, a szabadsághoz való jogot, vagy a lelkiismereti és vallásszabadságot.[18]

Egy incidens sokféle negatív hatással járhat az érintettek magánszférájára nézve, ebből sorol fel példálózó jelleggel néhányat a GDPR. Kockázatról többek között akkor beszélhetünk, ha 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. A természetes személyek jogait és szabadságait érintő kockázatok jelenthetnek hátrányos megkülönböztetést, személyazonosság-lopást vagy személyazonossággal való visszaélést, pénzügyi veszteséget, a jó hírnév sérelmét, a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülését, vagy bármilyen egyéb jelentős gazdasági vagy szociális hátrányt; vagy ha az érintettek nem gyakorolhatják jogaikat és szabadságaikat, vagy nem rendelkezhetnek saját személyes adataik felett.[19]

A kockázatelemzésnek objektív ismérveken kell alapulnia, illetve figyelembe kell venni a kockázatnak az érintett magánszférájára gyakorolt hatásának valószínűségét és súlyosságát.

Például, ha emberi hibából törlődik egy magán egészségügyi intézmény egészségügyi adatait tartalmazó adatbázisa, és a papír alapú nyilvántartásról történő helyreállás heteket vesz igénybe, amely következtében több műtéti beavatkozást is el kell halasztani, akkor az incidens az érintettek magánszférájára jelentős hatást gyakorolt. De például, ha egy hírlevél küldő szolgáltatónál a rossz beállítások miatt törlődnek az éles adatbázisból az érintettek személyes adatai, amelyet néhány napot követően helyreállítanak, eközben pedig az érintettek nem kapják meg a direkt-marketing üzeneteket, akkor az érintettek jogaira és szabadságaira az incidens nem gyakorolt hatást, nem járt kockázattal. De ha az utóbbi esetben a hírlevél küldő szolgáltatás a személyes adatokhoz egy zsarolóvírus támadás miatt nem fér hozzá ideiglenesen, de a zsaroló vírus nem csak titkosította, hanem el is lopta a személyes adatokat, akkor ez már kockázattal járhat az érintettek magánszférájára nézve.

3.2. Az adatvédelmi incidens kockázati besorolásánál figyelembe veendő szempontok és módszerek

A kockázatelemzés során érdemes mérlegelni az incidens típusát, az incidensben érintett személyes adatok kategóriáit, érzékenységét és számát. Fontos továbbá megvizsgálni, hogy az incidensben érintett adatalanyok mennyire egyszerűen azonosíthatók. Emellett vizsgálandó az incidens hatásainak a súlyossága, különösen, ha nagyszámú érintettre vagy sérülékenyebb érintetti körre gyakorol hatást az incidens. Végül fontos azt is figyelembe venni, ha az adatkezelő speciális tulajdonságából vonható le következtetés az érintettekre.

A kockázatok súlyosságát növelheti az incidens bekövetkezésének körülményei, az incidens típusa. Érzékenyebb adatok (például egészségügyi adatok, pénzügyi adatok) esetében elmondható, hogy az adatok jogosulatlan közlése vagy az ahhoz történő jogosulatlan hozzáférés többnyire nagyobb kockázat, mint az adatok véletlen törlése, különösen, ha az adatok – akár az érintett segítségével – helyreállíthatók.[20]

[18] WP250.

[19] GDPR (75) és (85) preambulumbekezdés.

[20] Péterfalvi et. al. 2018., 217-218.

A 29. cikk szerinti munkacsoport iránymutatásában kiemeli, hogy az incidens kockázatának megítélése különbözik az adatvédelmi hatásvizsgálat keretében történő felmérésétől. Míg az adatvédelmi hatásvizsgálat az adatkezelés végrehajtásának kockázataira és egy feltételezett incidens esetén felmerülő kockázatokra terjed ki, addig incidens esetén a már bekövetkezett esemény egyénekre gyakorolt hatását szükséges vizsgálni.[21]

Ugyanez az iránymutatás az alábbi szempontokat javasolja vizsgálni az incidens kockázatának megítélése során:

Az incidens jellege: Jelentősége lehet ugyanis annak, hogy az adatok elvesztek, vagy azokat jogosulatlan személye megismerték.

A személyes adatok jellege (típusa), érzékenysége és mennyisége: Általában minél érzékenyebbek az adatok, annál nagyobb a kár bekövetkeztének kockázata az érintett egyének számára, ugyanakkor ez esetenként eltérhet. (Például az egyén nevének és címének közlése, vagy az örökbefogadó szülő nevének és címének közlése.)

Ugyanígy fontos, hogy hány adat kerül ki az adott személyről, hiszen az egészségügyi adatokat, személyazonosító okmányokat vagy pénzügyi adatokat önmagukban is mind kárt okozhatnak, együttesen viszont már személyazonosság-lopáshoz vezethetnek, így együtt még nagyobb kockázatot jelentenek.

Az egyének könnyű azonosíthatósága: Fontos, hogy az érintetett az incidens folyamán mennyire könnyen lehet azonosítani közvetlenül a kikerült személyes adatok által, vagy az azokból levonható következtetéssel.

Az egyéneket érintő következmények súlyossága: A különleges kategóriájú adatok elvesztése például súlyosabban érintheti az érintetteket, mint az egyéb személyes adatokat ért incidens. A lehetséges kockázat magasabb, ha tudomással bír az adatkezelő arról, hogy rosszhiszemű személyek birtokába került a személyes adat, ugyanakkor enyhíti azt, ha az adatkezelő hatással lehet az adatok további sorsára, és jogosulatlanul megismerő személyt rábírja az adatok törlésére és/vagy visszajuttatására. Az egyéneket érintő következmények tartósságát is mérlegelni kell, amennyiben hosszan tartó hatások esetén súlyosabb az incidens kihatása.

Az egyén sajátosságai: Kiszolgáltatott helyzetben lévő személynek számító érintett esetén például a kockázat súlyosabbnak számít.

Az adatkezelő sajátosságai: Egy kórház különleges kategóriájú személyes adatokat dolgoz fel, következésképpen e személyes adataik megsértése esetén nagyobb fenyegetés éri az érintetteket.

Az érintett egyének száma: Minél nagyobb az érintettek száma, annál nagyobb az incidens kockázata.

A fentieket tehát együttesen javasolt értékelni és kétség esetén az adatkezelőnek a biztonság kedvéért érdemes inkább bejelentést tenni.[22]

Egy incidens kockázatelemzése során az egyik legfontosabb faktor az incidensben érintett személyes adatok érzékenységének a besorolása. Általánosságban kijelenthető, minél érzékenyebb adatokat érint az incidens, annál kockázatosabb a besorolása, ugyanakkor fontos figyelembe venni, hogy nyilvános vagy könnyen megismerhető személyes adatokkal kombinálható-e az incidensben érintett adatkör, hiszen ez jelentősen növelheti az incidens súlyosságát. Ugyancsak fontos tényező a kockázat besorolásánál, ha az adatból vagy adatok kombinációjából személyiségprofil építhető vagy érzékeny következtetés vonható le. Az incidensben érintett személyes adatok száma mint kockázatot befolyásoló tényező jelentősebb magyarázatot nem igényel. Kiemelendő, hogy fontos mindig esetről esetre vizsgálni a kockázatokat, de általánosságban kijelenthető, hogy minél több adatot és minél több fajtájú adatot érint az incidens, annál magasabb lehet a kockázati besorolása, hiszen annál pontosabb profil építhető az érintettről.

21 WP250, 24.

22 WP 250, 24-27.

A GDPR szövegéből közvetlenül következő kockázatbefolyásoló tényező az érintettek azonosíthatóságának a foka. Ennek a faktornak a mérlegelése csak az incidens körülményeinek az ismeretében lehetséges, hiszen könnyen előfordulhat, hogy az incidensben érintett adatok felhasználásával minden egyéb erőfeszítés nélkül közvetlenül azonosítható az érintett, de az is megtörténhet, hogy az érintettek azonosítása csak komoly erőfeszítések árán lehetséges. A természetes személyek azonosítása direkt vagy indirekt módon is megvalósulhat, ennek megítélése során figyelembe kell venni, hogy az érintett adatokból milyen következtetések vonható le, illetve mennyire kapcsolható össze nyilvánosan megismerhető adatokkal. Titkosítás, illetve pszeudoanonimizálás használata jelentősen csökkentheti ennek a kockázatnak a valószínűségét.

Az érintett kockázatainál mérlegelhető az a tényező is, mi vezetett az adatvédelmi incidenshez. Az esetek többségében egy rosszindulatú külső támadás esetén a kikerült személyes adatokkal való visszaélés valószínűsége magas. Ugyanakkor a kockázat valószínűsége csökkenthető, ha az incidens során olyan harmadik személy ismerte meg a személyes adatokat, amelynél az adatkezelő könnyen elérheti az incidens megfelelő kezelését. Például, ha emberi hiba miatt az adatkezelő egyik beszállítója ismeri meg a személyes adatokat, amely beszállítóval régóta szerződéses kapcsolatban van az adatkezelő, és a szerződésben szabályozott módon a beszállítónak dokumentálnia kell az adatkezelőt ért incidens mérséklésére tett lépéseket (dokumentált módon törli a jogellenesen megismert személyes adatokat), akkor a kikerült személyes adatokkal való visszaélés valószínűsége alacsony. Ugyancsak kockázatnövelő tényező, ha az incidensnek hosszútávú hatása lehet az érintettre. Kockázatnövelő tényező továbbá, ha az incidens kiszolgáltatott személyeket (például gyermekek) érint.

Általánosságban kimondható, minél magasabb az adatvédelmi incidenssel érintettek száma, annál súlyosabb az incidens. Ugyanakkor ezt a kritériumot sem lehet mechanikusan alkalmazni, hiszen egy érintett esetén is lehet az incidens olyan súlyosságú, hogy az incidens kockázatbesorolása magas lesz. Valamint sok érintett esetén is lehetnek olyan kockázatcsökkentő tényezők, amely alapján az incidens kockázatbesorolása alacsony marad.

Bizonyos esetekben az adatkezelő oldalán is lehet olyan kritériumot találni, amely emelheti az incidens besorolását, amikor magából az adatkezelőből lehet levonni bizonyos következtetéseket. Például önmagában a vásárlók listájának a nyilvánosságra kerülése nem magas kockázat, de ha ez egy daganatos megbetegedések kezelésére szolgáló étrendkiegészítő bolt vásárlóinak a listája, akkor az már magasabb kockázatot hordoz magában.

A kockázatelemzés során tehát az adatkezelőnek a fenti kritériumokat érdemes mérlegelnie és azokat figyelembe véve azonosítani az érintett jogaira és szabadságaira veszélyt jelentő kockázatokat, majd ezeket a kockázatokat valószínűség és súlyosság szerint besorolnia.

A fent említett szempontokat érdemes rendszerben, módszertan mentén elemezni. Egyelőre az Adatvédelmi Testület által is elfogadott módszertan erre nem létezik, de néhány kezdeményezés történt elemzési szempontok kidolgozására, amelyek segítséget nyújthatnak az adatkezelők számára.

A kockázat megítélésének bizonytalanságát felismerve az Európai Uniós Hálózat- és Információbiztonsági Ügynökség (ENISA) ajánlásokat fogalmazott meg az incidensek súlyosságának felmérésére szolgáló módszerről 2011-ben, majd ezt továbbfejlesztve a német és görög adatvédelmi hatóságokkal együttműködve 2013-ban kiadtak egy módszertant, ami bár a korábbi adatvédelmi irányelv alapján született, a jelenlegivel közel azonos szempontok szerint ítéli meg a kockázat besorolását.[23]

[23] Lásd: https://www.enisa.europa.eu/publications/dbn-severity (utolsó letöltés: 2019. október 16.)

A módszertan az értékelést az alábbi fő kritériumok mentén végzi:
- Az adatkezelés kontextusa (DPC): Az adatkezelés körülményeivel veti össze az incidenssel érintett adatokat.
- Az azonosíthatóság mértéke (EI): Azt állapítja meg, mennyire könnyű az azonosítás az incidensben érintett adatok által.
- Az incidens körülményei (CB): Az incidens körülményeit vizsgálja, így az adatok típusát, az adatbiztonság sérülését és a rosszhiszeműséget.

A módszertan az incidens súlyosságát a fenti indikátorok segítségével a következők szerint állapítja meg:

$$\text{Súlyosság} = \text{DPC} \times \text{EI+CB}$$

Ezt az értéket a 100 feletti érintett növeli, az adatok elérhetetlensége csökkenti. Az eredmény alacsony, közepes, magas vagy nagyon magas súlyú incidens lehet.

A módszertan ugyanakkor egy az egyben nem alkalmazandó a GDPR szerinti incidensek kockázati besorolására, inkább kiindulópontként szolgálhat, hiszen az egyik legfontosabb szempontot az incidensnek az érintettek magánszférájára gyakorolt hatását kevéssé veszi figyelembe.

Egy másik módszertan lehet a francia adatvédelmi hatóság általános kockázatelemző módszertana, amely négy kritériumrendszer köré szervezi a fentebb már említett szempontokat. Az adatkezelőnek először is vizsgálnia a kell a kockázat/incidens forrásait, amely elsősorban azt értékeli, mi vezetett az adatvédelmi incidenshez. Itt többnyire az kerül mérlegelésre, hogy külső vagy belső, illetve vétlen vagy rosszindulatú támadásról van szó. Egy belső vétlen hiba miatt bekövetkező incidens, például, ha egy munkavállaló véletlenül rossz címre küldi ki az e-mailt, alacsonyabb kockázati besorolású, mint egy külső rosszindulatú támadás, például, ha egy hackertámadás során megszereznek egy adatbázist. A második kritériumnál az adatkezelő azt mérlegeli, hogy milyen volt az adatkezelés környezete, ez többnyire az adatbiztonsági szint értékelését jelenti, amelynél mind a pozitív, mind a negatív körülményeket mérlegelni kell. Például, ha egy elavult titkosítási módszert használ az adatkezelő, akkor a kockázati besorolás magasabb, míg ha az adatkezelő például távolról törölni tudja az elhagyott eszközön lévő adatokat, akkor a kockázati besorolás alacsonyabb lesz. A harmadik kritérium az érintett személyes adatok elemzését tartalmazza, amely szempont elemzése fentebb már kifejtésre került. Tehát például magasabb kockázati besorolást kap az incidens, ha nagyszámú egészségügyi adatot érint, és alacsony besorolást kap, ha egy felhasználó e-mail címét érintette csak az incidens. A negyedik kritérium a lehetséges hatások, amelyek ugyancsak fentebb kifejtésre kerültek, így például magas kockázati besorolást eredményez, ha az incidens személyiséglopáshoz vagy vagyoni kárhoz vezet, míg alacsony a besorolása, ha az incidens egyetlen következménye az, hogy az érintett egy ideig nem kap direkt-marketing hírlevelet.

4. AZ ADATVÉDELMI INCIDENS NYILVÁNTARTÁSA

Az adatkezelő nyilvántartja az adatvédelmi incidenseket, feltüntetve az adatvédelmi incidenshez kapcsolódó tényeket, annak hatásait és az orvoslására tett intézkedéseket. E nyilvántartás lehetővé teszi, hogy a felügyeleti hatóság ellenőrizze a GDPR követelményeinek való megfelelést.[24]

A nyilvántartási kötelezettség valamennyi adatvédelmi incidensre kiterjed, függetlenül annak kockázataitól. Ez a kötelezettség elsősorban az elszámoltathatóság alapelvének az adatvédelmi incidensek kapcsán történő konkretizálása. A nyilvántartás formájára és módszerére a GDPR nem ad iránymutatást, az teljesen az adatkezelőtől döntésére bízza. Nagyobb adatkezelők esetén, ahol az adatvédelmi incidensek száma is vélhetőleg magasabb, érdemes ezt a nyilvántartást összekapcsolni az adatkezelési műveletek nyilvántartásával. Az elszámoltathatóság elvéből következik, hogy a fent leírtak mellett a nyilvántartásban érdemes azt is rögzíteni, hogy az adatkezelő milyen indokok alapján döntött az adatvédelmi incidens bejelentéséről, vagy annak mellőzéséről.

A korábbi hazai adatvédelmi szabályozás már tartalmazott hasonló kötelezettséget az adatkezelők számára, amikor kimondta, hogy az adatkezelő – ha belső adatvédelmi felelőssel rendelkezik, a belső adatvédelmi felelős útján – az adatvédelmi incidenssel kapcsolatos intézkedések ellenőrzése, valamint az érintett tájékoztatása céljából nyilvántartást vezet, amely tartalmazza az érintett személyes adatok körét, az adatvédelmi incidenssel érintettek körét és számát, az adatvédelmi incidens időpontját, körülményeit, hatásait és az elhárítására megtett intézkedéseket, valamint az adatkezelést előíró jogszabályban meghatározott egyéb adatokat.[25] Ennek megfelelően a GDPR fent említett rendelkezése nem számít újdonságnak a magyar adatkezelők számára.[26]

---

24 GDPR 33. cikk (5) bekezdés.
25 Infotv. 15. § (1a) bekezdés.
26 Péterfalvi et. al. 2018., 219.

5. AZ ADATVÉDELMI INCIDENS BEJELENTÉSE A FELÜGYELETI HATÓSÁGNAK

5.1. Az adatvédelmi incidens bejelentése a felügyeleti hatóságnak

Az adatvédelmi incidenst az adatkezelő indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, bejelenti az illetékes felügyeleti hatóságnak, kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Ha a bejelentés nem történik meg 72 órán belül, mellékelni kell hozzá a késedelem igazolására szolgáló indokokat is.[27]

A bejelentési kötelezettség tehát a tudomásszerzéstől és nem az incidens bekövetkezésétől jön létre. Tudomásszerzésnek az tekinthető, amikor az adatkezelő észszerű mértékű bizonyossággal rendelkezik arról, hogy olyan biztonsági esemény történt, amely személyes adatokkal kapcsolatos jogellenes műveletekhez vezethet. Hangsúly azon van, hogy az adatkezelő azonnali vizsgálatot kezdeményezzen annak megállapítására, hogy történt-e adatvédelmi incidens, és ha igen, milyen intézkedések szükségesek. Ennek a megelőző vizsgálatnak a hossza és bonyolultsága az adott incidens körülményeitől függ. Egyes esetekben gyorsan meg lehet állapítani, hogy incidens történt. Egy rossz címzettnek kiküldött e-mail esetében, ha a címzett visszajelez, hogy az e-mailt rossz e-mail-címre postázták, akkor azonnal ellenőrizhető az incidens ténye és körülményei. Más esetekben hosszabb vizsgálatra is szükség lehet. Például, ha egy újságíró keresi meg az adatkezelőt egy incidenssel kapcsolatosan, akkor egy rövid belső vizsgálatot le lehet folytatni, amely arra irányul, hogy az incidens valóban bekövetkezett-e. Ha az incidenst maga az adatkezelő azonosítja, például egy programozási vagy beállítási hiba feltárásával, akkor is egy rövid belső vizsgálatban érdemes felderíteni, hogy az adott hiba okán adatvédelmi incidens is történt-e az információbiztonsági incidens mellett.

Az értesülésnek, illetve a belső vizsgálat megkezdésének időpontjában még nem kell úgy tekinteni, hogy az adatkezelőnek tudomása van az incidensről, ugyanakkor fontos azt kiemelni, hogy a belső vizsgálatot azonnal el kell kezdeni és 72 órán belül be kell fejezni, ha eddig az időpontig nem tudott az adatkezelő kellő bizonyosságot szerezni az incidensről, akkor érdemes vélelmezni az incidens bekövetkeztét, és meg kell kezdeni az incidens bejelentését és kezelését.

Ezt az értelmezést erősíti az a lehetőség is, hogy az adatvédelmi incidens jelentés bármikor visszavonható. Ez a gyakorlatban gyakran előforduló forgatókönyv. Az adatvédelmi incidens vizsgálata során az adatkezelő juthat arra a következtetésre, hogy bár az elején incidensként vagy személyes adatokat érintő incidensként azonosította az eseményt, de végül kiderült, hogy nem történt incidens vagy az incidens nem érintett személyes adatokat.[28]

A bejelentésben az adatkezelőnek vagy a nevében eljáró adatfeldolgozónak ismertetni kell az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát. Közölni kell az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit. Ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket; továbbá az

---

27 GDPR 33. cikk (1) bekezdés.

28 Péterfalvi et. al. 2018., 220.

adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.[29]

Az adatvédelmi incidens bejelentés célja, hogy a természetes személyeknek esetlegesen okozott fizikai, vagyoni vagy nem vagyoni károkat az adatvédelmi incidens megfelelő és kellő idejű kezelésével csökkentse. Ennek megfelelően megakadályozza 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. A fent említett fogalmakat, mint például az érintettek kategóriái, az incidenssel érintett adatok kategóriái stb., ennek fényében érdemes bejelenteni. Ezzel összekapcsolva a bejelentett adatokat az elvégzett kockázatelemzéssel, tehát az érintettek kategóriái lehetnek ügyfelek; az incidenssel érintett adatok kategóriái elérhetőségei, pénzügyi és bankszámlaadatok; így ezek a bejelentett adatok egyértelműen hozzá kapcsolható olyan negatív kockázatokhoz, mint például személyazonossággal való visszaélés, pénzügyi veszteség stb.

A GDPR a minimálisan szolgáltatandó adatokat említi, az adatkezelő, ha rendelkezésére áll, több adatot is megadhat, továbbá az illetékes felügyeleti hatóság az incidensbejelentés alapján indított eljárása során további információkat kérhet az adatkezelőtől az incidenssel kapcsolatban.

Magyarországon az illetékes felügyeleti hatóság a NAIH, amely az incidensek bejelentésére online és offline formanyomtatványt tart fenn. Ebben a Hatóság a fent említett adatokat bekéri, tehát amennyiben az adatkezelő megfelelően kitölti a NAIH által közzétett adatlapot, akkor szolgáltatja a GDPR-ban előírt minimális adatokat.

A hatósági formanyomtatvány kitöltése során az adatkezelő az alábbi információkat szolgáltathatja:

- a bejelentő adatai (az adatkezelő adatai, ha van, akkor az adatvédelmi tisztviselő adatai, kapcsolattartó adatai);
- időpontok (az adatvédelmi incidens időpontja, az incidensről való tudomásszerzés időpontja);
- az incidens észlelésének módja; esetleges késedelmes tájékoztatás indokai;
- az adatvédelmi incidens jellege (például eszköz elvesztése vagy ellopása; informatikai rendszer feltörése; rosszindulatú számítógépes programok például zsarolóprogram; személyes adatok téves címzett részére történő elküldése stb.);
- az adatvédelmi incidenssel érintett személyes adatok (például azonosító adatok, pénzügyi adatok, különleges adatok);
- az adatvédelmi incidenssel érintett személyes adatok becsült száma; az érintettek kategóriái (például alkalmazottak, ügyfelek, kiskorúak stb.);
- az incidens előtt alkalmazott intézkedések; az incidens következményeinek a megjelölése (például bizalmas jelleg sérülése, integritás sérülése, rendelkezésre állás sérülése);
- az érintetteket ért fizikai, anyagi vagy nem vagyoni károk, vagy egyéb jelentős következmények, valamint a valószínűsíthető következmények súlyossága;
- a megtett intézkedések, ideértve az érintettek tájékoztatását – annak időpontját, formáját, tartalmát, a tájékoztatott érintettek számát, esetlegesen a tájékoztatás hiányának indokait;
- az adatvédelmi incidens orvoslására tett intézkedések; egyéb bejelentések (például az EU felügyeleti hatóságok listája, amelyeket az adatvédelmi incidens érinthet).

[29] GDPR 33. cikk (3) bekezdés.

Egy összetettebb adatvédelmi incidens esetén az adatkezelő az incidensről történt tudomásszerzést követő 72 órán belül általában nem rendelkezik valamennyi az incidensre vonatkozó adattal, így a bejelentésben sem tudja az összes adatot szolgáltatni. Ugyanakkor ez a tény nem akadályozhatja az adatkezelőt abban, hogy az incidenst – ha szükséges – 72 órán belül jelentse a felügyeleti hatóságnak. Ezt maga a GDPR is elismeri, hiszen ha és amennyiben nem lehetséges az információkat egyidejűleg közölni, azok további indokolatlan késedelem nélkül később részletekben is közölhetők.[30] Ennek megfelelően az adatkezelő az incidens további kivizsgálása során a tudomására jutott információkat később, folyamatosan megoszthatja a felügyeleti hatósággal.

Ha a bejelentés nem történik meg 72 órán belül, mellékelni kell hozzá a késedelem igazolására szolgáló indokokat is. A szabályozás tehát megengedi az adatkezelő számára, hogy ha a bejelentésre rendelkezésre álló szűk határidőt elmulasztja, akkor kimentheti magát. A kimentési indokokról a szabályozás nem szól, de az incidens jelentés természetéből adódóan méltánylandó kimentő ok lehet, ha az adatkezelő azért nem tudta a bejelentést időben megtenni, mert az incidens megfékezésével, a kárenyhítéssel volt elfoglalva. Ha egy incidens során az adatkezelő teljes IT infrastruktúrája használhatatlanná válik, akkor az adatkezelőnek először a jogszerű működést kell helyreállítani, ennek keretében az érintetteket érő károkat kell enyhíteni, és csak utána szükséges a felügyeleti hatóságot értesíteni.

A GDPR 33. cikk (1) bekezdése értelmében, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve, akkor az adatvédelmi incidenst nem kell bejelenteni a felügyeleti hatóságnak. Például, ha az adatkezelőtől a személyes adatok megfelelően erősen titkosított formában, álnevesítve kerültek ki és létezik biztonsági mentés, amelyből az adatok visszaállítható, akkor az incidens valószínűsíthetően nem hordoz kockázatot az érintett magánszférájára nézve.[31]

Az adatvédelmi incidenst az adatkezelő a GDPR 55. cikke alapján illetékes felügyeleti hatóságnak jelenti be. Határon átnyúló adatkezelés esetén, illetve ha az adatvédelmi incidens több tagállamban is érint adatalanyokat, a felügyeleti hatóság meghatározása nagyobb jelentőséggel bír. A GDPR 55. cikk (1) bekezdése alapján a felügyeleti hatóság a saját tagállamának területén illetékes a rendelet alapján ráruházott feladatok végzésére és hatáskörök gyakorlására. A GDPR 56. cikk (1) bekezdése szerint az 55. cikk sérelme nélkül, az adatkezelő vagy az adatfeldolgozó tevékenységi központja vagy egyetlen tevékenységi helye szerinti felügyeleti hatóság jogosult fő felügyeleti hatóságként eljárni az említett adatkezelő vagy az adatfeldolgozó által végzett határokon átnyúló adatkezelés tekintetében, a 60. cikk szerinti eljárással összhangban. A GDPR 56. cikk (6) bekezdése értelmében pedig a fő felügyeleti hatóság az adatkezelő vagy adatfeldolgozó egyetlen kapcsolattartója az általuk végzett, határokon átnyúló adatkezeléssel kapcsolatban. Mindez azt jelenti, ha az adatvédelmi incidens több tagállamban is érint adatalanyokat, akkor az adatkezelő az adatvédelmi incidenst a vezető felügyeleti hatóságnak jelenti be. Ugyanakkor, ha az adatvédelmi incidens más tagállamban lévő leányvállalatot is érint, vagy egy másik tagállam polgárait is érinti, ajánlott, hogy az adatkezelő ezt az információt a vezető felügyeleti hatóságnak jelezze. A NAIH fent említett formanyomtatványán erre egyébiránt lehetőséget biztosít.

A bejelentésben ismertetni kell az adatvédelmi incidens jellegét, az érintettek kategóriáit és számát, valamint a személyes adatok kategóriáit és számát; az adatvédelmi tisztviselő vagy egyéb kapcsolattartó nevét és elérhetőségeit; a valószínűsíthető következményeket; és a megtett vagy tervezett intézkedéseket. Ha ez nem lehetséges, az információk részletekben is közölhetők.[32]

[30] GDPR 33. cikk (4) bekezdés.
[31] Péterfalvi et. al. 2018., 221.
[32] GDPR 33. cikk (3) és (4) bekezdés.

5.2. A Hatóság incidenskezelési felületének ismertetése

Az adatvédelmi incidens bejelentést az adatkezelő a NAIH által erre a célra fenntartott elektronikus felületen vagy papír alapon (az erre szolgáló formanyomtatványon) tudja bejelenteni. A papír alapú formanyomtatvány teljes egészében az elektronikus felület által szolgáltatandó adatokat tartalmazza.

A Hatóság honlapján elérhető elektronikus felület regisztrációval és anélkül is igénybe vehető.

A bal felső „incidens bejelentése" fülön keresztül lehet adatvédelmi incidenst bejelenteni. Ki kell választani, hogy milyen minőségben kívánjuk megtenni a bejelentést, ezt követően az adatvédelmi incidens bejelentés típusa esetén kiválasztható a teljes bejelentés, szakaszos bejelentés, és lehetőség van a bejelentés módosítására (visszavonására) is.

A következő oldalon a „bejelentő adatkezelő" adatait kell megadni. A bejelentési felületen ki kell választani a bejelentés idejét, az adatkezelő megnevezését, a bejelentőt, a bejelentés státuszát. Nyilatkozni kell az adatvédelmi tisztviselő, vagy további tájékoztatást nyújtó személy és a bejelentő azonosságáról, amennyiben nem azonos a személy, úgy a rá vonatkozó kapcsolattartási adatokat is meg kell adni. Amennyiben az adatkezelőn kívül más személy (például adatfeldolgozó) is részt vesz az incidenssel érintett szolgáltatásban, a rá vonatkozó adatokat is meg kell adni.

Az „időpontok" rögzítésénél az „adatvédelmi incidens időpontja", „az incidensről való tudomásszerzés időpontja" megadása kötelező óra, perc pontossággal. Az adatvédelmi incidensről való tudomásszerzés időpontja nem lehet korábbi, mint az adatvédelmi incidens – bekövetkezési – időpontja.

„Az incidens észlelésének módja" szabadszavas mezőben lehet az incidens észlelésének körülményeit kifejteni. Indokolt esetben az adatfeldolgozó általi észlelés időpontját és egyéb megjegyzéseket is lehet írni az incidens időpontját érintően.

Az „adatvédelmi incidensről" szóló fül alatt a „sérülés jellege" résznél lehet kiválasztani a bizalmas jelleg, integritás, rendelkezésre állás kategóriákat (akár többet is).

Az „Adatvédelmi incidens jellege" résznél:

- az eszköz elvesztése vagy ellopása;
- papír alapú dokumentum elvesztése, ellopása, vagy olyan helyen hagyása amely minősül biztonságosnak;
- levél elvesztése vagy jogosulatlan felnyitása;
- informatikai rendszer feltörése (hackelés);
- rosszindulatú számítógépes programok például zsarolóprogram, vírus;
- adathalászat;
- papír alapú dokumentum nem megfelelő módon történő megsemmisítése;
- elektronikus hulladék (a személyes adatok rajta maradnak az elavult eszközön);
- személyes adatok nagy nyilvánosság előtti jogellenes közzététele;
- személyes adatok jogosulatlan megismerése;
- személyes adatok téves címzettek részére történő elküldése;
- személyes adatok jogosulatlan szóbeli közlése;
- egyéb kategóriák közül választhatunk, illetve több is választható.

Az „Adatvédelmi incidens leírása" résznél szabadszavas mezőben lehet összefoglalni az adatvédelmi incidenst. Az adatkezelőknek ebben a részben érdemes a legrészletesebben leírni, mi történt az incidens során.

Az „Adatvédelmi incidens okai” alatt:
- a szervezeten belüli, rosszhiszeműnek nem minősülő cselekmény;
- szervezeten belüli, rosszhiszemű cselekmény;
- külső rosszhiszeműnek nem minősülő cselekmény;
- külső rosszhiszemű cselekmény;
- egyéb kategóriák közül választhatunk, illetve több is választható

„Az incidenssel érintett személyes adatok” fül alatt „Az adatvédelmi incidenssel érintett személyes adatok jellege” résznél:
- a személyazonossághoz kapcsolódó adatok;
- elérhetőségi adatok;
- azonosító adatok;
- személyi szám;
- hivatalos okmányok;
- helymeghatározó adatok;
- gazdasági, pénzügyi adatok;
- büntetett előélettel, bűncselekményekkel vagy büntetéssel, intézkedéssel kapcsolatos adatok;
- különleges adatok;
- illetve több is megadható.

A „Különleges adatok” megadása körében:
- faji eredetre, nemzetiséghez tartozásra vonatkozó adatok;
- politikai véleményre vonatkozó adatok;
- vallásos vagy más világnézeti meggyőződésre vonatkozó adatok;
- érdek-képviseleti szervezeti tagságra vonatkozó adatok;
- szexuális életre vonatkozó adatok/ egészségügyi adatok;
- genetikai adatok;
- biometrikus adatok;
- még nem ismert;
- egyéb kategóriák közül választhatunk, illetve több is választható .

Emellett „Az adatvédelmi incidenssel érintett személyes adatok becsült száma” résznél lehet megadni, mennyi személyes adatot érintett az incidens.

„Az érintettek” fül alatt az „Érintettek jellege” résznél:
- alkalmazottak;
- felhasználók;
- feliratkozók;
- diákok;
- katonai állomány tagjai;
- ügyfelek (jelenlegi és pontenciális) ;
- páciensek;
- kiskorúak;
- kiszolgáltatott személyek;
- hatósági eljárás vagy intézkedés alá vont, vagy azok által érintett személyek;
- még nem ismert;
- egyéb kategóriák közül választhatunk, illetve több is választható.

Ezt követően az incidenssel érintett adatalanyok részletes leírása résznél lehet pontosítani az érintetteket. Az adatvédelmi incidenssel érintettek becsült számánál pedig az adható meg, mennyi érintettre jelent kockázatot az incidens.

„Az incidens ELŐTT alkalmazott intézkedések” résznél „Az adatvédelmi incidens előtt alkalmazott intézkedések leírása” cím alatt foglalható össze, hogy milyen szervezési, technikai intézkedések végrehajtására került sor az adatvédelmi incidenst megelőzően.

A „Következmények” résznél a „Bizalmas jelleg sérülése” cím alatt:
- a szélesebb körű hozzáférés, mint ami szükséges, vagy amihez az érintett hozzájárult;
- az adat összekapcsolhatóvá vált az érintett egyéb adatával;
- Az adatot más célokból történő, tisztességtelen módon történő kezelése lehetséges

kategóriák közül lehet választani, illetve több is választható.

Az „Integritás sérülése” cím alatt az adat módosíthatóvá vált annak ellenére, hogy:
- archivált elavult adat volt;
- az adatot valószínűsíthetően módosították, egyébként pontos adatokra, és azokat eltérő célokra használták;
- egyéb kategóriák közül választhatunk, illetve több is választható.

A „rendelkezésre állás sérülése” cím alatt:
- az érintettek számára történő szolgáltatásnyújtás képességének elvesztése;
- az érintettek számára történő kritikus szolgáltatásnyújtás képességének módosulása;
- egyéb kategóriák közül választhatunk, illetve több is választható.

„Az érintetteket ért fizikai, anyagi vagy nem vagyoni károk, vagy egyéb jelentős következmények” résznél „Az incidens valószínűsíthető hatásai az érintettekre” cím alatt:
- személyes adatok feletti rendelkezés elvesztése;
- érintett jogainak korlátozása/ hátrányos megkülönböztetés;
- személyazonosság-lopás;
- személyazonossággal való visszaélés;
- pénzügyi veszteség;
- álnevesítés engedély nélküli feloldása;
- jó hírnév sérelme;
- szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülése;
- egyéb kategóriák közül választhatunk, illetve több is választható.

„A valószínűsíthető következmények súlyossága cím alatt:
- elhanyagolható;
- jelentős;
- maximális kategóriák közül választhatunk;
- illetve csak egy választható.

A „Megtett intézkedések” résznél az „Érintettek tájékoztatása” címnél:
- igen/nem;
  - o de az érintettek tájékoztatva lesznek,
  - o nem, nem lesz tájékoztatás,
  - o nem tudja kategóriák közül lehet választani.

A tájékoztatás esetén annak időpontját és a tájékoztatott érintettek számát és a tájékoztatás formáját is meg kell adni, továbbá az érintetteknek szóló tájékoztatás tartalma cím alatt a tájékoztatót is el kell helyezni. Amennyiben tervezik a tájékoztatást, úgy annak dátumát meg lehet adni, vagy a tájékoztatás tervezett időpontja még nincs eldöntve mező melletti checkboxban kell nyilatkozni. Amennyiben nem lesz tájékoztatás, úgy a tájékoztatás hiányának indokai közül ki kell választani, hogy:

- az adatkezelő megfelelő technikai és szervezési intézkedéseket hajtott végre és ezeket az intézkedéseket az adatvédelmi incidens által érintett adatok tekintetében alkalmazták, különösen olyan intézkedéseket, amelyek a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik azokat;
- 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 érintettek egyenkénti tájékoztatása aránytalan erőfeszítést tenne szükségessé az adatkezelő számára.

„Az adatvédelmi incidens orvoslására tett intézkedések" mezőben lehet kifejteni az orvoslás körében tett intézkedéseket. Az „Egyéb bejelentések" cím alatt:
- a vezető hatóságoknak bejelentett határokon átnyúló adatvédelmi incidens;
- az adatkezelő bejelentette-e, vagy be fogja-e jelenteni az adatvédelmi incidenst közvetlenül más tagállam felügyeleti hatóságának;
- bejelentette-e, vagy be fogja-e jelenteni az adatkezelő az adatvédelmi incidenst az Unión kívüli adatvédelmi hatóságnak;
- bejelentette-e, vagy be fogja-e jelenteni az adatkezelő az adatvédelmi incidenst egyéb uniós hatóságnak egyéb jogszabály alapján fennálló kötelezettség alapján;
- bejelentette-e, vagy be fogja-e jelenteni az adatkezelő az adatvédelmi incidenst másik EGT-tagállam olyan adatkezelőjének, amely részére az incidenssel érintett adatokat korábban továbbította, vagy amely adatkezelő az incidenssel érintett adatokat részére átadta kategóriák közül lehet választani.

Fontos kiemelni, hogy a NAIH által rendszeresített formanyomtatvány kitöltése már önmagában egy alapos áttekintést ad az adatvédelmi incidensről. Ennek megfelelően az adatkezelőknek az adatvédelmi incidensek bejelentésére vonatkozó kötelezettségére jó felkészülést jelent, ha a formanyomtatványt megismerik, illetve belső folyamataikat úgy építik fel, hogy a formanyomtatvány gyors kitöltését meg tudják valósítani.

5.3. A Hatóság adatvédelmi incidensekkel kapcsolatos eljárása

A NAIH-hoz eddig körülbelül 700 incidensbejelentés érkezett. A Hatóság incidensbejelentés esetén az Ákr. VI. fejezete által szabályozott hatósági ellenőrzés keretében jár el. Ennek megfelelően amennyiben az egyszeri vagy szakaszos bejelentés nem tartalmaz minden szükséges információt, a Hatóság a tényállás tisztázása érdekében felveszi a kapcsolatot az adatkezelővel. A hatósági ellenőrzés a GDPR 33-34. cikkében foglalt kötelezettségek betartását vizsgálja, melytől a 32. cikkben foglaltak nem választhatók el élesen, így a vizsgálat arra is kiterjedhet. A hatósági ellenőrzés végén jogsértés esetén a Hatóság eljárást indít, míg ellenkező esetben a hatósági ellenőrzést lezárja.

A hatósági eljárás lezárásakor a felügyeleti hatóság mérlegelheti a korrekciós intézkedések alkalmazását, ezen belül bírság kiszabását egy intézkedés helyett vagy mellett.[33] Fontos azonban, hogy amennyiben egy ilyen eljárásban fény derül arra, hogy az adatbiztonsági intézkedések hiányosak, vagy nem megfelelők, úgy az incidens bejelentésének vagy az arról való tájékoztatásnak az elmulasztása, másrészt a (megfelelő) biztonsági intézkedések hiánya miatt is lehetősége van szankciókat alkalmazni, mivel ezek két különálló jogsértésnek minősülnek.[34]

[33] GDPR 58. cikk (2).
[34] WP250, 9-10.

Különleges esete az incidensek kivizsgálásával kapcsolatos eljárásoknak a határon átnyúló adatkezeléssel kapcsolatos incidensekhez fűződő eljárás. A GDPR 56. cikke értelmében ilyenkor az adatkezelő vagy az adatfeldolgozó tevékenységi központja vagy egyetlen tevékenységi helye szerinti felügyeleti hatóság jogosult fő felügyeleti hatóságként eljárni, míg a többi érintett tagállam hatósága véleményezhetik a fő felügyeleti hatóság döntés tervezetét, ahhoz megjegyzéseket, vagy kifogásokat fűzhetnek. Erre tekintettel az adatkezelőnek javasolt beazonosítani azt a fő felügyeleti hatóságot, aki felé az incidensbejelentést meg kell tenni. Az ilyen bejelentés során azonban jelezni kell, hogy az incidens más tagállamokban található tevékenységi helyeket is érint, és valószínűsíthetően mely tagállamokban van hatással az incidens érintettekre. Ha kétséges a fő felügyeleti hatóság kiléte, úgy azon felügyeleti hatóságának kell bejelentést tenni, ahol az incidens történt.[35]

Az incidens azonosítását, hatásainak feltérképezését, nyilvántartás vezetését, a felügyeleti hatóság értesítésének és az érintett tájékoztatásának fontosságát külön kiemeli a GDPR (87) preambulum bekezdése, amely szerint meg kell bizonyosodni arról, hogy az összes megfelelő technológiai védelmi és szervezési intézkedés végrehajtásra került-e, egyrészt az adatvédelmi incidens haladéktalan megállapítása, másrészt a felügyeleti hatóságnak történő bejelentés és az érintett sürgős értesítése érdekében. Azt, hogy az értesítésre 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.

Ha az adatkezelő nem teljesíti a fent említett kötelezettségeit, akkor a felügyeleti hatóság gyakorolhatja a GDPR-ban meghatározott korrekciós hatásköreit, amely magába foglalja annak a lehetőségét is, hogy közigazgatási bírságot szab ki. A bírság mértéke legfeljebb 10 millió euró, illetve a vállalkozások esetében az előző pénzügyi év teljes éves világpiaci forgalmának legfeljebb 2%-át kitevő összeg; a kettő közül a magasabb összeget kell kiszabni.

[35] WP250, 18.

6. AZ ÉRINTETT TÁJÉKOZTATÁSA AZ ADATVÉDELMI INCIDENSRŐL

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.[36]

Az érintett részére adott tájékoztatásban világosan és közérthetően ismertetni kell:
- az adatvédelmi incidens jellegét, és legalább közölni kell az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;
- az adatvédelmi incidensből eredő, valószínűsíthető következményeket;
- az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.[37]

Az érintett számára nyújtott tájékoztatási kötelezettség feltétele magasabb, mint a felügyeleti hatóság számára történő bejelentés során, ugyanis az adatvédelmi incidensnek magas kockázattal kell járnia az érintett jogaira és szabadságaira nézve. Ugyanakkor, bár az esetek egy részében nem kell, de érdemes az érintettet az adatvédelmi incidensről tájékoztatni, hiszen ebben az esetben az érintett is bevonható az incidens kockázatainak a mérséklésébe, amely csökkenti az incidens általános kockázati értékét.

A tájékoztatást közvetlenül az érintettnek kell megküldeni, kivéve, ha a tájékoztatás aránytalan erőfeszítést tenne szükségessé. Ilyen esetekben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, vagy olyan hasonló intézkedést kell hozni, amely biztosítja az érintettek hasonlóan hatékony tájékoztatását.

A tájékoztatásnak egyedinek kell lennie, azaz csak az adatvédelmi incidenssel kapcsolatos információkat tartalmazhat, az nem vonható össze egyéb tájékoztatásokkal, nem történhet hírlevélben vagy frissítési információkkal együtt, hiszen ezekben az esetekben a tájékoztatás világosságához és közérthetőségéhez kétség férhet.

A tájékoztatás közérthetőségéhez hozzátartozik, amennyiben az elektronikus formában történik, akkor azt közismert formátumot használva kell megtenni, hogy az érintett is meg tudja nyitni a tájékoztatást. Továbbá, ha ez ismert, akkor a tájékoztatást az érintett anyanyelvén, vagy ennek hiányában az érintett által preferált nyelven kell megtenni.

A tájékoztatás során figyelemmel kell lenni arra, hogy az adatkezelő ne használja az incidensben esetleg érintett kommunikációs csatornákat addig, amíg annak biztonságáról meg nem bizonyosodott.[38]

A tájékoztatást indokolatlan késedelem nélkül kell megtenni, és a fent említett kötelező elemek mellett mindig érdemes az érintettet tájékoztatni arról, mit tehet az incidens hatásainak csökkentése érdekében. Az érintettek tájékoztatásáról az észszerűség keretei között a lehető leghamarabb gondoskodni kell, szorosan együttműködve a felügyeleti hatósággal, és betartva az általa vagy más érintett hatóságok például bűnüldöző hatóságok által adott útmutatást.[39]

---

36 GDPR 34. cikk (1) bekezdés.
37 GDPR 34. cikk (2) bekezdés.
38 Péterfalvi et. al. 2018., 223.
39 GDPR (86) preambulumbekezdés.

Az érintettet nem kell tájékoztatni, ha a következő feltételek bármelyike teljesül:

- 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;
- 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;
- a tájékoztatás aránytalan erőfeszítést tenne szükségessé.

Ilyen esetekben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, vagy olyan hasonló intézkedést kell hozni, amely biztosítja az érintettek hasonlóan hatékony tájékoztatását.[40]

Ha 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, vagy megállapíthatja valamelyik előbb említett feltétel teljesülését.[41]

Fontos kiemelni, ha az adatkezelő, amellett döntött, hogy az érintetteket nem tájékoztatja az incidensről, vagy azért, mert az nem jár magas kockázattal, vagy azért, mert a fent említett feltételek valamelyike teljesül, akkor az adatkezelőnek az elszámoltathatóság alapelvéből következően ezt a döntését megfelelően dokumentálni és indokolni kell, illetve a felügyeleti hatóság kérésére az indokokat ismertetni szükséges.

[40] GDPR 34. cikk (3) bekezdés.
[41] GDPR 34. cikk (4) bekezdés.

7. AZ ADATVÉDELMI INCIDENS KEZELÉSÉNEK BELSŐ ELJÁRÁSRENDJE

7.1. Az adatvédelmi incidens kezelési szabályzat és az adatvédelmi incidens kezelő csoport

A gyors és sikeres incidenskezelés egyik előfeltétele a megfelelő felkészültség. Nem várható el sikeres reagálás egy incidensre, ha az adatkezelő preventív szemlélettel nem gondolja végig a lehetséges eseményeket és az erre adandó válasz lépéseit belső szabályzatban vagy belső eljárásrendben nem rögzíti. A belső szabályozásban érdemes előre meghatározni, milyen módszertan alapján, milyen szempontok figyelembevételével fog történni a kockázatok azonosítása. Az incidenst milyen infrastruktúrán és kik fogják vizsgálni, mikor kerül sor külső szakértők bevonására. Az incidens kezelés során hogyan történik a felső vezetés értesítése és bevonása az incidens kezelésébe; illetve az adatvédelmi tisztviselő hogyan válik az incidens kezelés részévé. A belső szabályozás elsődleges célja, hogy az incidens kezelése gördülékenyen haladjon, a szabályzatok segítséget nyújthatnak az incidens kezelésében részt vevőknek, hogy megállapíthassák, milyen eljárásrendet kell követni, milyen lépéseket kell megtenni (például mikor és kit kell értesíteni), ki a felelős az adott eljárásért, ki és milyen intézkedésre jogosult.

Egy incidens kezelése során bevett eljárás incidenskezelő csoport (incident response team) felállítása. A csoport tevékenységének és eljárásrendjének a szabályozása azért kiemelt jelentőségű, mert nem elvárható egy ad hoc, hirtelen felállított és felkészületlen csapattól, hogy sikeresen reagáljon egy incidensre. A csoport szabályozása során az adatkezelőnek érdemes áttekintenie adatkezeléseit és azonosítani azokat a területeket, amelyeket egy adatvédelmi incidens érinthet (például IT, HR, ügyfélszolgálat, felső vezetők). A csoportra vonatkozó belső szabályozásban definiálhatja az adatkezelő a csapat által elérendő célokat. Az adatkezelő képességeitől függően ez irányulhat csupán az incidens azonosítására, az incidens megfékezésére és jelentésére, az incidenshez kapcsolódó bizonyítékok dokumentálására, az incidenshez vezető okok feltárására és esetlegesen kijavítására, illetve akár a teljes incidens kivizsgálására. Ha a csoportban részt vevő munkatársakat előre meghatározta a belső eljárásrend, akkor az incidensek kezelésére felkészítő oktatás is könnyebben megszervezhető. A szabályozásnak természetesen rugalmasnak és dinamikusan skálázhatónak kell lennie, hogy a különböző súlyú és volumenű incidensekre reagálni tudjon, illetve nyitva kell hagyni a külső szakértők bevonásának a lehetőségét. Természetesen az adatkezelő lehetőségeihez és az incidensek gyakoriságához mérten állandó jelleggel is üzemelhet incidenskezelő csoport.

Az incidens kezelések során a belső eljárásrend mellett a külső szereplőkkel történő kommunikációra is fel kell készülnie az adatkezelőnek. Az incidensek során ilyen kommunikációs elvárás az adatfeldolgozóval, a felügyeleti hatósággal, az érintettekkel és a külső szakértőkkel való kommunikáció.[42]

---

[42] Péterfalvi et. al. 2018., 224.

7.2. Az adatvédelmi tisztviselő szerepe az adatvédelmi incidensek kezelésében

Ha az adatkezelő adatvédelmi tisztviselőt nevezett ki, akkor rá az incidens kezelésében jelentős szerep hárul. A GDPR alapjában véve kapcsolattartási és koordinációs szerepet szán neki a folyamatban, ugyanakkor egy általános szupervizori szerep alkalmasabb megközelítés.

7.3. Az adatfeldolgozó kötelezettségei az adatvédelmi incidensekkel kapcsolatosan

Bár az általános felelősség az adatvédelmi incidensek kezeléséért, bejelentéséért az adatkezelőt terheli, az esetek egy jelentős részében az adatfeldolgozónak is jelentős lehet a szerepe. Ez a GDPR-ból is következik, hiszen az adatfeldolgozásra irányuló szerződésben (vagy egyéb jogi aktusban) szabályozni kell, hogy az adatfeldolgozó hogyan segíti az adatkezelőt az adatvédelmi incidensekkel kapcsolatos kötelezettségeinek a teljesítésében; különös tekintettel a rendelkezésre álló információk átadásában.[43]

Az adatfeldolgozó az adatvédelmi incidenst, az arról való tudomásszerzést követően indokolatlan késedelem nélkül bejelenti az adatkezelőnek.[44]

A GDPR pontos határidőt nem határoz meg, de a rendszertani elemzés alapján megállapítható, hogy az adatfeldolgozónak 72 órán belül kell az adatkezelőt értesítenie. Tekintettel arra, hogy az adatfeldolgozó az adatkezelő nevében kezeli a személyes adatokat, így az adatfeldolgozó tudomásszerzésével az adatkezelő is tudomást szerzett az incidensről, és a 72 órás határidő számítása megkezdődik. Ennek megfelelően az adatfeldolgozónak olyan módon kell az adatkezelőt értesítenie, hogy az még teljesíteni tudja a GDPR 33-34. cikkében előírt kötelezettségeit.

Ha az adatfeldolgozó több adatkezelő számára is nyújt hasonló szolgáltatást és az incidens az adatfeldolgozó érdekkörében merült fel, akkor az adatfeldolgozónak valamennyi adatkezelőt külön-külön kell értesítenie. Az adatfeldolgozó az adatkezelő nevében is megteheti a legfontosabb kötelezettségeket (például bejelentheti az incidenst a felügyeleti hatóságnak, tájékoztathatja az érintetteket az incidensről), ha erre megfelelő felhatalmazással rendelkezik az adatkezelőtől. Megemlítendő ugyanakkor, hogy a GDPR alapján a jogi kötelezettség az adatkezelőt terheli, ennek megfelelően az adatfeldolgozó mulasztása az adatkezelőt fogja terhelni.[45]

[43] GDPR 28. cikk (3) bekezdés f) pont.
[44] GDPR 33. cikk (2) bekezdés.
[45] Péterfalvi et. al. 2018., 225.

8. ADATVÉDELMI INCIDENS BEJELENTÉSE A BŰNÜGYI ADATVÉDELMI IRÁNYELV ÉS AZ INFOTV. ALAPJÁN

Az adatvédelmi reform kapcsán megszületett egy másik jogszabály, az Európai Parlament és a Tanács (EU) 2016/680 irányelve (2016. április 27.) a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről (a továbbiakban: bűnügyi adatvédelmi irányelv) is tartalmaz az adatvédelmi incidensekkel kapcsolatos előírásokat, amelyet az Infotv. módosításával implementált a hazai jogalkotó.

Az Infotv. továbbá a fenti irányelv hatálya alá nem tartozó nemzetbiztonsági célú adatkezelések tekintetében is bevezette az adatvédelmi incidensek kezelésére és bejelentésére szolgáló rezsimet.

Az Infotv. 25/J. és 25/K. § szabályozza e tevékenységek során az adatvédelmi incidensek kezelését. Maga a szabályozás a GDPR-ban fentebb ismertetett szabályok megismétlése kisebb eltérésekkel. Ennek megfelelően az ilyen esetekben is a fent leírtaknak megfelelően kell az adatvédelmi incidenseket kezelni.

Fontos kiegészítő szabály, hogy ha az adatvédelmi incidens során olyan adat érintett, amelyet valamely más EGT-állam adatkezelője továbbított az adatkezelő részére, vagy amelyet az adatkezelő más EGT-állam adatkezelője részére továbbított, az adatvédelmi incidens bejelentést az adatkezelő ezen EGT-állam adatkezelőjével haladéktalanul közli.

A bejelentési kötelezettséget az adatkezelő – a minősített adatot tartalmazó bejelentés kivételével – a Hatóság által e célra biztosított elektronikus felületen teljesíti. Tehát ebben az esetben a papír alapú bejelentésnek csak kivételes esetben van helye.

Nemzetbiztonsági célú adatkezelés esetén az általános szabályokat azzal az eltéréssel kell alkalmazni, hogy ha az adatkezelő bejelentési, illetve a tájékoztatási kötelezettsége nemzetbiztonsági érdekbe ütközne, azt e nemzetbiztonsági érdek megszűnését követően kell teljesíteni.

Ha magas kockázatú adatvédelmi incidens történt, akkor az adatkezelő – a nemzetbiztonsági célú adatkezelés kivételével – az érintettet az adatvédelmi incidensről haladéktalanul tájékoztatja. Az adatkezelő mentesül az érintett tájékoztatásának kötelezettsége alól, ha:

a) az adatkezelő az adatvédelmi incidenssel érintett adatok tekintetében az adatvédelmi incidenst megelőzően megfelelő – így különösen az adatokat a jogosulatlan személy általi hozzáférés esetére értelmezhetetlenné alakító, azok titkosítását eredményező – műszaki és szervezési védelmi intézkedéseket alkalmazott;
b) az adatkezelő az adatvédelmi incidensről való tudomásszerzését követően alkalmazott intézkedésekkel biztosította, hogy az adatvédelmi incidens folytán az érintettet megillető valamely alapvető jog érvényesülését lényegesen befolyásoló következmények valószínűsíthetően nem következnek be;
c) az érintett közvetlen tájékoztatása csak az adatkezelő aránytalan erőfeszítésével lenne teljesíthető, ezért az adatkezelő az érintettek részére az adatvédelmi incidenssel összefüggő megfelelő tájékoztatást bárki által hozzáférhető módon közzétett információk útján biztosítja;
d) vagy törvény a tájékoztatást kizárja.

9. IRODALOMJEGYZÉK

1. Péterfalvi Attila – Révész Balázs – Buzás Péter (szerk.) (2018): Magyarázat a GDPR-ról. Wolters Kluwer, Budapest.
2. Jóri András – Soós Andrea (2016): Adatvédelmi jog. HVG-ORAC, Budapest.
3. A Nemzeti Adatvédelmi és Információszabadság Hatóság beszámolója a 2016. évi tevékenységéről. Elérhetőség: https://www.naih.hu/files/NAIH-BESZ-MOL--2016_Mid-Res.pdf (utolsó letöltés: 2019. szeptember 15.)
4. A Nemzeti Adatvédelmi és Információszabadság Hatóság beszámolója a 2017. évi tevékenységéről. Elérhetőség: https://www.naih.hu/files/NAIH-BESZAMOLO-2017-mid-res.pdf (utolsó letöltés: 2019. szeptember 15.)
5. A Nemzeti Adatvédelmi és Információszabadság Hatóság beszámolója a 2018. évi tevékenységéről. Elérhetőség: https://www.naih.hu/files/Beszamolo-2018-MR.PDF (utolsó letöltés: 2019. szeptember 15.)
6. A 29. cikk szerinti munkacsoport iránymutatása az adatvédelmi incidensek (EU) 2016/679 rendelet szerinti bejelentéséről (a továbbiakban: WP250). Elérhetőség: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052 (utolsó letöltés: 2019. szeptember 15.)

A Nemzeti Közszolgálati Egyetem kiadványa.

Nemzeti Közszolgálati Egyetem;
Közigazgatási Továbbképzési Intézet
www.uni-nke.hu

Felelős Kiadó:
Prof. Dr. Kis Norbert rektorhelyettes

Címe:
1083 Budapest, Üllői út 82.

Kiadói szerkesztő:
Császár-Biró Anna

Tördelőszerkesztő:
Friebert Máté

ISBN 978-963-498-207-4 (elektronikus)