A 29. cikk SZERINTI ADATVÉDELMI MUNKACSOPORT

18/HU

WP250rev.01

Iránymutatás az adatvédelmi incidensek (EU) 2016/679 rendelet szerinti bejelentéséről

Elfogadás időpontja: 2017. október 3.

A legutóbbi felülvizsgálat és elfogadás időpontja: 2018. február 6., kedd

AZ EGYÉNEKNEK A SZEMÉLYES ADATOK FELDOLGOZÁSA TEKINTETÉBEN VALÓ VÉDELMÉVEL FOGLALKOZÓ MUNKACSOPORT

amelyet az 1995. október 24-i 95/46/EK európai parlamenti és tanácsi irányelvvel hoztak létre,

tekintettel az említett irányelv 29. és 30. cikkére,

tekintettel eljárási szabályzatára,

ELFOGADTA EZT AZ IRÁNYMUTATÁST:

TARTALOMJEGYZÉK TOC

BEVEZETÉS

A természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról szóló rendelet (a továbbiakban: az általános adatvédelmi rendelet) bevezeti azt a követelményt, miszerint minden adatvédelmi incidenst (a továbbiakban: incidens) be kell jelenteni a nemzeti felügyeleti hatóságnak[1] (vagy több országot érintő incidens esetén a fő hatóságnak), és egyes esetekben tájékoztatni kell azokat az egyéneket, akiknek a személyes adatait az incidens érinti.

Az incidensek bejelentésére vonatkozó kötelezettségek jelenleg bizonyos szervezeteket, köztük (a 2009/136/EK irányelvben és a 611/2013/EU rendeletben foglaltak szerint[2]) a nyilvánosan elérhető elektronikus hírközlési szolgáltatást nyújtó szolgáltatókat terhelik. Az uniós tagállamok egy része már előírt saját nemzeti incidensbejelentési kötelezettséget. E körbe tartozik a nyilvánosan elérhető elektronikus hírközlési szolgáltatást nyújtó szolgáltatókon túlmenően a meghatározott kategóriákba tartozó adatkezelőket érintő incidensek bejelentésére vonatkozó kötelezettség (például Németországban és Olaszországban) vagy a személyes adatokat érintő összes incidens bejelentésének kötelezettsége (például Hollandiában). Más tagállamok erre vonatkozó eljárási szabályzattal rendelkeznek (például Írország[3]). Noha jelenleg több uniós adatvédelmi hatóság is az incidensek jelentésére biztatja az adatkezelőket, az 95/46/EK adatvédelmi irányelv[4], amelynek a helyébe az általános adatvédelmi rendelet lép, nem rögzít külön incidensbejelentési kötelezettséget, ezért az ilyen jellegű követelmény sok szervezet számára újdonság lesz. Az általános adatvédelmi rendelet viszont az összes adatkezelő számára kötelezően előírja a bejelentést, kivéve, ha az incidens valószínűsíthetően nem jár kockázattal az egyének jogaira és szabadságaira nézve[5]. Az adatfeldolgozók szintén fontos szerepet töltenek be, hiszen ők is kötelesek bármilyen incidenst jelenteni az adatkezelőjüknek[6].

A 29. cikk szerinti munkacsoport úgy véli, hogy az új bejelentési követelménynek több előnnyel is jár. Ha bejelentést tesznek a felügyeleti hatóságnak, az adatkezelők tanácsot kaphatnak azzal kapcsolatosan, hogy tájékoztatniuk kell-e az érintett egyéneket. Sőt, a felügyeleti hatóság utasíthatja is az adatkezelőt, hogy tájékoztassa az érintett egyéneket az incidensről[7]. Az adatkezelő az egyének incidensről való tájékoztatása keretében felvilágosítást nyújthat arról, milyen kockázatok merülnek fel az incidens miatt, és mely intézkedésekkel védekezhetnek az egyének a lehetséges következményekkel szemben. Az incidenskezelési terveknek mindenekelőtt az egyének és az ő személyes adataik védelmére kell irányulnia. Következésképpen az incidensbejelentést a személyes

[1] Lásd az általános adatvédelmi rendelet 4. cikkének 21. pontját.

[2] Lásd: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=celex:32009L0136 és https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A32013R0611

[3] Lásd: https://www.dataprotection.ie/docs/Data_Security_Breach_Code_of_Practice/1082.htm

[4] Lásd: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=celex:31995L0046

[5] Az Európai Unió Alapjogi Chartájában rögzített jogok; a Charta a következő internetcímen érhető el: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:12012P/TXT

[6] Lásd a 33. cikk (2) bekezdését. Ez a rendelkezés tartalmilag hasonló a 611/2013/EU rendelet 5. cikkéhez, miszerint az elektronikus hírközlési szolgáltatás egy részének nyújtásával megbízott, az előfizetőkkel közvetlen szerződéses jogviszonyban nem álló szolgáltató a személyes adatok megsértése esetén köteles az őt megbízó szolgáltatót haladéktalanul értesíteni.

[7] Lásd a 34. cikk (4) bekezdését és az 58. cikk (2) bekezdésének e) pontját.

adatok védelmével kapcsolatos előírások betartást előmozdító eszköznek kell tekinteni. Egyúttal megjegyzendő, hogy az egyén incidensről való értesítésének vagy az incidens felügyeleti hatóságnak való bejelentésének elmulasztása esetén előfordulhat, hogy a 83. cikk értelmében esetleg szankciót kell alkalmazni az adatkezelővel szemben.

Az adatkezelőket és az adatfeldolgozókat ezért arra biztatjuk, hogy előre alakítsanak ki és vezessenek az incidensek észlelésére és mielőbbi elhárítására alkalmas eljárásokat, mérjék fel az egyéneket érintő kockázatot[8], majd ennek alapján állapítsák meg, hogy szükséges-e bejelentést tenni az illetékes felügyeleti hatóságnak, és szükség esetén tájékoztassák az érintett egyéneket az incidensről. A felügyeleti hatóságnak történő bejelentésnek az említett incidenskezelési terv részét kell képeznie.

Az általános adatvédelmi rendelet rendelkezéseket tartalmaz arra vonatkozóan, mikor és kinek kell bejelenteni az incidenst, és milyen információkat kell közölni a bejelentésben. A bejelentéshez szükséges információk részletekben is megadhatók, de az adatkezelőknek minden esetben időben kell intézkedniük az incidens kezeléséről.

A személyes adatok megsértése bejelentéséről szóló 03/2014 sz. véleményében[9] a 29. cikk szerinti munkacsoport iránymutatást nyújtott az adatkezelőknek, hogy könnyebben eldönthessék, értesítsék-e az érintetteket incidens esetén. A vélemény az elektronikus hírközlési szolgáltatásokat nyújtó szolgáltatóknak a 2002/58/EK irányelvből fakadó kötelezettségeire vonatkozik, több ágazatból hozott fel példákat az akkor még csak tervezetként létező általános adatvédelmi rendelettel összefüggésben, és bevált gyakorlatokat mutatott be minden adatkezelő számára.

A mostani iránymutatás felvilágosítást nyújt az általános adatvédelmi rendeletben rögzített incidensbejelentési és tájékoztatási követelményekről és ezzel összefüggésben ismertet néhány, az adatkezelők és az adatfeldolgozók által az új kötelezettségeik teljesítése érdekében hozható intézkedést. Mindemellett példákon keresztül ismerteti az incidensek különböző fajtáit és azt, hogy különféle esetekben kit kell értesíteni.

I. Adatvédelmi incidensek bejelentése az általános adatvédelmi rendelet szerint

A. Alapvető biztonsági szempontok

Az általános adatvédelmi rendelet egyik követelménye szerint a személyes adatok kezelését oly módon kell végezni, hogy a 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[10].

Az általános adatvédelmi rendelet ennek megfelelően az adatkezelőktől és az adatfeldolgozóktól egyaránt megköveteli, hogy megfelelő technikai és szervezési intézkedéseket hajtsanak végre a kezelt személyes adatokat érintő kockázat mértékének megfelelő szintű adatbiztonság garantálása érdekében. Ennek során figyelembe kell venniük a tudomány és technológia állását és a megvalósítás

[8] A természetes személyek jogaira és szabadságaira nézve valószínűsíthetően magas kockázattal járó adatkezelési műveletek esetén szükséges adatvédelmi hatásvizsgálatra vonatkozó nyomonkövetési és ellenőrzési követelmény alapján biztosítható (a 35. cikk (1) és (11) bekezdése).

[9] Lásd a személyes adatok megsértése bejelentéséről szóló 03/2014 sz. véleményt: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp213_hu.pdf

[10] Lásd az 5. cikk (1) bekezdésének f) pontját és a 32. cikket.

költségeit, továbbá az adatkezelés jellegét, hatókörét, körülményeit és céljait, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázatot[11]. Az általános adatvédelmi rendelet azt is előírja, hogy az összes megfelelő technológiai védelmi és szervezési intézkedést végre kell hajtani annak haladéktalan megállapítása céljából, hogy történt-e incidens, ugyanis ettől függ, hogy életbe lép-e a bejelentési kötelezettség[12].

Következésképpen minden adatbiztonsági politika esetében döntő jelentősége van annak, hogy az incidensek lehetőség szerint megelőzhetőek legyenek, és amennyiben mégis bekövetkeznek, időben lehessen válaszintézkedéseket hozni.

B. Mi az adatvédelmi incidens?

1. Fogalommeghatározás

Az incidensek kezelésére irányuló bármilyen kísérlet első lépéseként az adatkezelőnek fel kell tudnia ismerni az ilyen eseteket. Az általános adatvédelmi rendelet a 4. cikkének 12. pontjában a következőképpen határozza meg az „adatvédelmi incidens” fogalmát:

> „az adatbiztonság olyan sérelme, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, módosítását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi”.

Teljesen egyértelmű, mit értünk a személyes adatok „megsemmisítése” alatt: az az eset, amikor az adatok egyáltalán nem, vagy az adatkezelő számára nem használható formában léteznek. A „károsodás” fogalma is viszonylag egyértelmű: az az eset, amikor a személyes adatok módosultak, sérültek, vagy már nem hiánytalanok. A személyes adatok „elvesztése” úgy értelmezendő, hogy az adatok még léteznek, de az adatkezelő már nem rendelkezik felettük, nem fér hozzájuk, vagy azok nincsenek a birtokában. Végezetül pedig jogosulatlan vagy jogellenes adatkezelésnek minősülhet a személyes adatok közlése (vagy hozzáférhetővé tétele) arra jogosulatlan címzettek számára, illetve bármilyen egyéb, az általános adatvédelmi rendeletbe ütköző adatkezelés.

Példa

A személyes adat elvesztése merülhet fel például abban az esetben, ha az adatkezelő ügyféladatbázisának példányát tartalmazó készülék elveszik, vagy ellopják azt. Az adatok elvesztésére másik példa, ha a személyes adatok állományából létező egyetlen példányt zsarolóvírus titkosítja, vagy az adatkezelő titkosította, de a titkosításhoz használt kulcs már nincs a birtokában.

Világosan látni kell, hogy az adatvédelmi incidens egyfajta biztonsági incidens. Azonban a 4. cikk 12. pontja is kifejezi, hogy az általános adatvédelmi rendelet csak azokra az esetekre vonatkozik, amikor a *személyes adatok* biztonsága sérül. Az ilyen jellegű incidens következménye, hogy az adatkezelő nem tudja biztosítani azoknak a személyes adatok kezelésére vonatkozó elveknek a betartását, amelyeket az általános adatvédelmi rendelet 5. cikke rögzít. Ebben nyilvánul meg a különbség a biztonsági incidens és az adatvédelmi között: lényegét tekintve minden adatvédelmi

[11] 32. cikk; lásd még a (83) preambulumbekezdést.

[12] Lásd a (87) preambulumbekezdést.

incidens biztonsági incidens, azonban nem feltétlenül minősül mindegyik biztonsági incidens adatvédelmi incidensnek[13].

Az alábbiakban azzal foglalkozunk, milyen hátrányos hatásokat gyakorolhatnak az adatvédelmi incidensek az egyénekre.

2. Az adatvédelmi incidensek fajtái

A személyes adatok megsértése bejelentéséről szóló 03/2014 sz. véleményében a 29. cikk szerinti munkacsoport kifejtette, hogy az adatvédelmi incidensek az alábbi három jól ismert információbiztonsági elv[14] szerint kategorizálhatók:

- „titoksértés”: személyes adatok jogosulatlan vagy véletlen közlése vagy az ilyen adatokhoz való jogosulatlan vagy véletlen hozzáférés;
- „sértetlenségi adatsértés”: személyes adatok jogosulatlan vagy véletlen módosítása;
- „hozzáférhetőségi adatsértés”: a személyes adatokhoz való hozzáférés[15] véletlen vagy jogosulatlan elvesztése vagy a személyes adatok véletlen vagy jogosulatlan megsemmisítése.

Megjegyzendő, hogy az incidens a körülményektől függően egyidejűleg vagy bármilyen kombinációban érintheti a személyes adatok titkosságát, sértetlenségét és hozzáférhetőségét.

Míg a titoksértés vagy a sértetlenségi adatsértés viszonylag egyértelműen megállapítható, addig a hozzáférhetőségi adatsértés már kevésbé nyilvánvaló. Az incidens mindig hozzáférhetőségi adatsértésnek minősül, ha a személyes adatok véglegesem elvesznek vagy megsemmisülnek.

Példa

A hozzáférhetőség elveszéséhez vezethet például az adatok véletlen törlése, jogosulatlan személy általi törlése vagy biztonságosan titkosított adatok esetében a visszafejtő kulcs elveszítése. Amennyiben az adatkezelő nem tudja helyreállítani – például biztonsági másolatból – az adatokhoz való hozzáférést, akkor ez a hozzáférhetőség végleges elveszésének tekinthető.

A hozzáférhetőség akkor is elveszhet, ha jelentős zavar keletkezik a szervezet rendes működésében, például áramkimaradás vagy a szolgáltatás megtagadásával járó támadás miatt válnak elérhetetlenné a személyes adatok.

[13] Megjegyzendő, hogy a biztonsági incidens fogalma nem korlátozódik azokra a fenyegetési modellekre, amikor a szervezetet külső forrásból éri támadás, hanem azokra az incidensekre is kiterjed, amikor a belső adatkezelés ütközik a biztonsági elvekbe.

[14] Lásd a 03/2014 sz. véleményt.

[15] Általánosan elfogadott, hogy a „hozzáférés” elengedhetetlen a „hozzáférhetőséghez”. Lásd például az Egyesült Államok Nemzeti Szabványügyi és Technológiai Intézetének (National Institute of Standards and Technology, NIST) SP800-53rev4 számú dokumentumát, amely a következőképpen határozza meg a „hozzáférhetőség” fogalmát: „az információkhoz való hozzáférés biztosítása időben és megbízható módon”; a dokumentum a következő internetcímen érhető el: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf. A CNSSI-4009 számú utasítása szintén említést tesz a hozzáférhetőségről: „Időszerű, megbízható hozzáférés az adat- és információs szolgáltatásokhoz engedéllyel rendelkező felhasználók számára.” See https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf. Az ISO/IEC 27000:2016 szabványban szereplő fogalommeghatározás szerint a „hozzáférhetőség” szintén „az arra jogosult általi, igény szerinti hozzáférés és felhasználás lehetősége”. Lásd: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-4:v1:en

Felmerül a kérdés, hogy a személyes adatok hozzáférhetőségének átmeneti elveszése is adatvédelmi incidensnek tekintendő-e, és ha igen, be kell-e jelenteni. Az általános adatvédelmi rendelet „Az adatkezelés biztonsága” című 32. cikke szerint a kockázat mértékének megfelelő szintű adatbiztonságot garantáló technikai és szervezési intézkedések végrehajtásakor mérlegelni kell többek között „a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítását, integritását, rendelkezésre állását és ellenálló képességét”, valamint „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”.

Következésképpen a személyes adatok bizonyos időre hozzáférhetetlenné válását eredményező biztonsági incidens is egyfajta adatvédelmi incidens, mivel az adatokhoz való hozzáférés hiánya jelentős kihatással lehet a természetes személyek jogaira és szabadságaira. A tisztánlátás érdekében le kell szögezni, hogy nem minősül a 4. cikk 12. pontjában meghatározott „adatvédelmi incidensnek”, ha a személyes adatok tervezett rendszerkarbantartás miatt nem hozzáférhetőek.

A személyes adatok végleges elvesztéséhez vagy megsemmisüléséhez (sőt, minden egyéb jellegű adatvédelmi incidenshez) hasonlóan a hozzáférhetőség átmeneti elveszésével járó incidensekről a 33. cikk (5) bekezdése szerint nyilvántartást kell vezetni. Az adatkezelő ezáltal könnyebben tudja bizonyítani elszámoltathatóságát a felügyeleti hatóság előtt, amely betekintést kérhet ebbe a nyilvántartásba[16]. Azonban az adatvédelmi incidens körülményeitől függ, hogy szükséges-e bejelentést tenni a felügyeleti hatóságnak, és tájékoztatni az érintett egyéneket. Az adatkezelőnek fel kell mérnie a személyes adatok hozzáférhetetlensége miatt a természetes személyek jogaira és szabadságaira gyakorolt hatás valószínűségét és súlyosságát. A 33. cikk szerint az adatkezelőnek bejelentést kell tennie, kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal az egyének jogaira és szabadságaira nézve. Ezt természetesen eseti alapon kell értékelni.

Példák

Ha kórházi környezetben a betegek létfontosságú egészségügyi adatai, még ha ideiglenesein is, de nem férhetők hozzá, ez kockázatot jelenthet az egyének jogaira és szabadságaira nézve, például előfordulhat, hogy műtéteket kell elhalasztani, és emberéletek kerülhetnek veszélybe.

Ezzel szemben akkor, ha egy médiavállalkozás rendszerei válnak több órára hozzáférhetetlenné (például áramkimaradás miatt), valószínűsíthetően nem jár kockázattal az egyének jogaira és szabadságaira nézve, hogy a vállalkozás nem tud hírlevelet küldeni a feliratkozóinak.

Megjegyzendő, hogy noha az adatkezelő rendszereinek hozzáférhetősége csak átmenetileg veszhet el, és ez talán nincs is kihatással az egyénekre, az adatkezelőnek mégis fontos mérlegelnie az incidens összes lehetséges következményét, mivel előfordulhat, hogy más okokból bejelentést kell tennie.

Példa

A zsarolóvírussal (az adatkezelő adatait váltságdíj fizetéséig titkosító, rosszindulatú szoftverrel) való fertőzés a hozzáférhetőség átmeneti elveszéséhez vezethet, amennyiben az adatok biztonsági másolatból helyreállíthatók. Mindazonáltal ezzel hálózati behatolás történt, és bejelentésre lehet szükség, ha az incidens titoksértésnek minősül (vagy a támadó személyes adatokhoz fért hozzá), ami kockázatot jelent az egyének jogaira és szabadságaira nézve.

3. Az adatvédelmi incidensek lehetséges következményei

[16] Lásd a 33. cikk (5) bekezdését

Az adatvédelmi incidenseknek különféle, jelentősen hátrányos hatásai lehetnek az egyénekre, ezek a hatások pedig fizikai, vagyoni vagy nem vagyoni károkhoz vezethetnek. Az általános adatvédelmi rendelet szerint ilyen kár lehet többek között a személyes adataik feletti rendelkezés elvesztése vagy a jogaik korlátozása, a hátrányos megkülönböztetés, a személyazonosság-lopás vagy a személyazonossággal való visszaélés, a pénzügyi veszteség, az álnevesítés engedély nélküli feloldása, a jó hírnév sérelme, valamint a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülése. E körbe tartozik még az egyéneket sújtó egyéb jelentős gazdasági vagy szociális hátrány is[17].

Az általános adatvédelmi rendelet ennek megfelelően megköveteli, hogy az adatkezelő jelentse be az adatvédelmi incidenseket az illetékes hatóságnak, kivéve, ha valószínűsíthetően nem merül fel az említett hátrányos hatások kialakulásának kockázata. Arra az esetre, ha valószínűleg nagy az e hátrányos hatások kialakulásának kockázata, az általános adatvédelmi rendelet előírja, hogy az adatkezelő az észszerűség keretei között a lehető leghamarabb tájékoztassa az érintett egyéneket[18].

Az incidensek felismerése, az egyéneket érintő kockázat felmérése, majd pedig a szükség szerinti értesítés iránti képesség fontosságát az általános adatvédelmi rendelet (87) preambulumbekezdése is hangsúlyozza:

> „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. A felügyeleti hatóságnak történt bejelentést az e rendeletben meghatározott feladataival és hatásköreivel összhangban történő beavatkozását eredményezheti."

Az egyéneket érintő hátrányos hatások kockázatának felméréséről további iránymutatás a IV. szakaszban található.

Ha az adatkezelők a 33., illetve a 34. cikkben megfogalmazott követelmények teljesülése ellenére nem tesznek bejelentést az adatvédelmi incidensről a felügyeleti hatóságnak, az érintetteknek vagy senkinek sem, akkor a felügyeleti hatóság választás előtt áll, amelynek keretében mérlegelnie kell a rendelkezésére álló összes korrekciós intézkedést, többek között megfelelő közigazgatási bírság kiszabását[19] önmagában vagy az 58. cikk (2) bekezdésében szereplő egyik korrekciós intézkedés kiegészítéseként. Amennyiben a hatóság a közigazgatási bírság kiszabása mellett dönt, annak összege az általános adatvédelmi rendelet 83. cikke (4) bekezdésének a) pontja szerint legfeljebb 10 000 000 EUR vagy a vállalkozás előző pénzügyi évi teljes világpiaci forgalmának legfeljebb 2%-a lehet. Szintén fontos szem előtt tartani, hogy az incidens bejelentésének elmulasztása bizonyos esetekben fényt deríthet a biztonsági intézkedések hiányára vagy a meglévő biztonsági intézkedések elégtelenségére. A 29. cikk szerinti munkacsoport közigazgatási bírság alkalmazásáról és megállapításáról szóló iránymutatása szerint: „Amennyiben egyetlen konkrét ügyben számos együtt elkövetett különböző jogsértés fordul elő, a felügyeleti hatóságnak lehetősége van arra, hogy olyan mértékű közigazgatási bírságot szabjon ki, amely a legsúlyosabb jogsértés korlátain belül hatékony, arányos és visszatartó erejű." Ebben az esetben a felügyeleti hatóságnak egyrészt az incidens

[17] Lásd még a (85) és (75) preambulumbekezdést.

[18] Lásd még a (86) preambulumbekezdést.

[19] Részletesebb felvilágosítást a 29. cikk szerinti munkacsoport közigazgatási bírság alkalmazásáról és megállapításáról szóló iránymutatása nyújt, amely a következő internetcímen érhető el: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889

bejelentésének vagy az arról való tájékoztatásnak (33. és 34. cikk) az elmulasztása, másrészt a (megfelelő) biztonsági intézkedések (32. cikk) hiánya miatt is lehetősége van szankciókat alkalmazni, mivel ezek két különálló jogsértésnek minősülnek.

II. 33. cikk – Bejelentés a felügyeleti hatóságnak

A. Mikor kell bejelentést tenni?

1. A 33. cikkben rögzített követelmények

A 33. cikk (1) bekezdése a következőképpen rendelkezik:

> „Az adatvédelmi incidenst az adatkezelő indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, bejelenti az 55. cikk alapján 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.”

A (87) preambulumbekezdés a következőket mondja ki[20]:

> „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. A felügyeleti hatóságnak történt bejelentést az e rendeletben meghatározott feladataival és hatásköreivel összhangban történő beavatkozását eredményezheti.”

2. Mikor jut az adatvédelmi incidens az adatkezelő „tudomására”?

A fentiekben kifejtettek szerint az általános adatvédelmi rendelet előírja, hogy az incidenst az adatkezelő köteles indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az incidens a tudomására jutott, bejelenteni. Ezzel kapcsolatosan felmerülhet a kérdés, hogy mikor tekinthető úgy, hogy az incidens az adatkezelő „tudomására” jutott. A 29. cikk szerinti munkacsoport álláspontja szerint akkor tekinthető úgy, hogy az incidens az adatkezelő „tudomására” jutott, amikor az adatkezelő észszerű bizonyossággal meggyőződött arról, hogy olyan biztonsági incidens történt, amelynek következtében a személyes adatok veszélybe kerültek.

Azonban az általános adatvédelmi rendelet a fent leírtak szerint megköveteli, hogy az adatkezelő az összes megfelelő technikai védelmi és szervezési intézkedést végrehajtsa, egyrészt az incidens haladéktalan megállapítása, másrészt a felügyeleti hatóságnak történő bejelentés és az érintettek sürgős értesítése érdekében. Emellett rögzíti, hogy azt, hogy az értesítésre indokolatlan késedelem nélkül került-e sor, különösen az incidens jellegére és súlyosságára, valamint annak az érintettre gyakorolt következményeire, illetve hátrányos hatásaira figyelemmel kell megállapítani[21]. Ezzel kötelezettséget ír elő az adatkezelő számára a tekintetben, hogy időben szerezzenek „tudomást” az esetleges incidensekről, mivel így tudják megtenni a megfelelő intézkedést.

[20] Ehhez kapcsolódóan a (85) preambulumbekezdés is fontos.

[21] Lásd a (87) preambulumbekezdést.

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

Példák

1. Titkosítatlan személyes adatokat tartalmazó USB-kulcs elvesztése esetén gyakran nem lehet meggyőződni arról, hogy jogosulatlan személyek hozzáfértek-e az adatokhoz. Mindazonáltal, még ha az adatkezelő nem is tudja megállapítani, hogy sérült-e az adatok bizalmas jellege, az incidenst akkor is be kell jelenteni, mivel észszerű bizonyossággal állítható, hogy sérült a hozzáférhetőség. Az adatkezelőnek ez az eset akkor jut „tudomására”, amikor fény derül arra, hogy az USB-kulcs elveszett.

2. Harmadik fél arról tájékoztatja az adatkezelőt, hogy véletlenül a birtokába jutottak az adatkezelő egyik ügyfelének személyes adatai, és a jogosulatlan közlést bizonyítékkal is alátámasztja. Mivel az adatkezelő egyértelmű bizonyítékot kapott a tekinteben, hogy sérült az adatok bizalmas jellege, így kétségtelenül a „tudomására” jutott.

3. Az adatkezelő észleli, hogy lehetséges, hogy behatoltak a hálózatába. Ellenőrzi rendszereit annak megállapítása érdekében, hogy a bennük tárolt személyes adatok sérültek-e, és adott esetben ezt megállapítja. Az adatkezelőnek ez esetben is egyértelmű bizonyítéka van az incidens megtörténtére, így kétségtelenül a „tudomására” jutott.

4. Kiberbűnöző keresi meg az adatkezelőt, hogy váltságdíjat követeljen tőle, miután feltörte a rendszerét. Ebben az esetben, miután az adatkezelő meggyőződött arról, hogy rendszerét valóban támadás érte, egyértelmű bizonyítéka van az incidens megtörténtére, így az kétségtelenül a „tudomására” jutott.

Amikor az adatkezelő egyéntől, médiaszervezettől vagy más forrásból először értesül esetleges adatvédelmi incidensről, vagy saját maga észlel biztonsági incidenst, rövid vizsgálatot folytathat annak megállapítása érdekében, hogy valóban sérültek-e adatok. E vizsgálat ideje alatt nem tekinthető úgy, hogy az adatkezelő „tudomására” jutott az incidens. Ugyanakkor az első vizsgálatot minél előbb meg kell kezdeni, és észszerű bizonyossággal meg kell állapítani, hogy történt-e incidens. Ezután folytatható mélyrehatóbb vizsgálat.

A bejelentési kötelezettség alá tartozó incidenst az adatkezelő tudomására jutása után indokolatlan késedelem nélkül, és ha lehetséges, 72 órán belül be kell jelenteni. Ez idő alatt az adatkezelőnek fel kell mérnie az egyéneket valószínűleg érintő kockázatot annak megállapítása céljából, hogy fennáll-e az értesítési követelmény, és milyen intézkedést vagy intézkedéseket kell tenni az adatok sérelmének kezelése érdekében. Azonban előfordulhat, hogy az adatkezelő az érintett adatkezelési művelet végrehajtása előtt lefolytatott adatvédelmi hatásvizsgálat[22] keretében már végzett előzetes felmérést az incidens következtében esetlegesen felmerülő kockázatról. Ugyanakkor az adatvédelmi hatásvizsgálat általánosabb jellegű lehet a ténylegesen bekövetkezett incidens konkrét körülményeihez képest, így minden esetben kiegészítő felmérést kell végezni e körülmények figyelembevételével. A kockázatok felméréséről részletesebb felvilágosítás a IV. szakaszban olvasható.

[22] Lásd a 29. cikk szerinti munkacsoport adatvédelmi hatásvizsgálatokról szóló iránymutatását itt: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137

A legtöbb esetben ezeket az előzetes intézkedéseket nem sokkal az első figyelmeztető jelzés után (vagyis amikor az adatkezelőnél vagy az adatfeldolgozónál felmerül a gyanú, hogy esetlegesen személyes adatokat érintő biztonsági incidens történhetett) végre kell hajtani. Több időt csak kivételes esetekben lehet erre fordítani.

Példa

Egy egyén arról tájékoztatja az adatkezelőt, hogy magát az adatkezelőnek kiadó személytől kapott e-mailt, amely személyes adatokat tartalmaz arról, hogyan vette (ténylegesen) igénybe az adatkezelő szolgáltatását, ami arra utal, hogy az adatkezelőnél veszélybe került a biztonság. Az adatkezelő rövid vizsgálatot folytat, amelynek során feltárja, hogy hálózatába behatoltak, és bizonyítékot talál a személyes adatokhoz való jogosulatlan hozzáférésre. Ezzel úgy tekinthető, hogy az incidens az adatkezelő „tudomására" jutott, és be kell jelenteni a felügyeleti hatóságnak, kivéve, ha valószínűsíthetően nem jár kockázattal az egyének jogaira és szabadságaira nézve. Az adatkezelőnek megfelelő korrekciós intézkedéseket kell tennie az incidens kezelésére.

Az adatkezelőnek ezért rendelkeznie kell belső eljárásokkal, hogy észlelni és kezelni tudja az incidenseket. Ha például szabálytalanságokat fedez fel az adatkezelésben, akkor az adatkezelő vagy az adatfeldolgozó bizonyos technikai megoldásokat, például adatáramlás- és naplóelemző programokat használhat, amelyekkel a rendelkezésre álló naplóadatok[23] összevetése alapján események és figyelmeztető jelzések határozhatók meg. Fontos, hogy incidens észlelése esetén értesíteni kell a megfelelő vezetési szinten lévő felettest, hogy az incidenst kezelni és szükség szerint jelenteni lehessen a 33. és – adott esetben – a 34. cikknek megfelelően. Az ilyen intézkedések és jelentési mechanizmusok részletesen meghatározhatók az adatkezelő incidenskezelési tervében, illetve irányítási rendjében. Ezek segítségével az adatkezelő hatékonyan tervezhet, és meghatározhatja, hogy a szervezeten belül ki visel operatív felelősséget az incidensek kezeléséért, adott esetben a felettes elé kell-e utalni az incidenst, és ha igen, hogyan.

Az adatkezelőnek emellett megállapodással kell rendelkezniük az általuk igénybe vett adatfeldolgozókkal, akik incidens esetén maguk is kötelesek értesíteni az adatkezelőt (lásd lent).

Ugyan az adatkezelők és az adatfeldolgozók feladata, hogy olyan alkalmas intézkedéseket vezessenek be, amelyekkel megelőzhetik az incidenseket, reagálhatnak rájuk, és kezelhetik őket, azonban bizonyos gyakorlati lépést minden esetben meg kell tenni.

- A biztonságot érintő összes eseményről tájékoztatni kell a felelős személyt vagy személyeket, akinek vagy akiknek a feladata az incidensek kezelése, az adatvédelmi incidens bekövetkeztének megállapítása és a kockázat felmérése.
- Ezután fel kell mérni az incidens következtében az egyéneket érintő kockázatot (a kockázatmentesség, a kockázat és a jelentős kockázat valószínűsége), egyúttal tájékoztatni kell a szervezet érintett részlegeit.
- Szükség esetén az incidensről bejelentést kell tenni a felügyeleti hatóságnak, és esetleg tájékoztatni kell az érintett egyéneket.
- Az adatkezelőnek egyúttal gondoskodnia kell az incidens elhárításáról, majd a helyreállításról.
- Az incidens alakulásáról nyilvántartást kell vezetni.

[23] Megjegyzendő, hogy a például az adatok tárolásának, módosításának vagy törlésének ellenőrzését megkönnyítő naplóadatok szintén személyes adatnak minősülhetnek az adott feldolgozási műveletet kezdeményező személy vonatkozásában.

Ennek megfelelően egyértelműnek kell lennie, hogy az adatkezelő köteles intézkedni az első figyelmeztető jelzés alapján, és megállapítani, hogy valóban történt-e incidens. E rövid idő alatt az adatkezelőnek lehetősége van arra, hogy valamilyen vizsgálatot folytasson, valamint bizonyítékokat és más lényeges részleteket gyűjtsön. Azonban azt követően, hogy az adatkezelő észszerű bizonyossággal megállapította az incidens megtörténtének tényét, a 33. cikk (1) bekezdésében rögzített feltételek teljesülése esetén indokolatlan késedelem nélkül, és ha lehetséges, 72 órán belül bejelentést kell tennie a felügyeleti hatóságnak[24]. Ha az adatkezelő nem intézkedik időben, és nyilvánvalóvá válik, hogy incidens történt, akkor ez az eset a 33. cikk szerinti bejelentés elmulasztásának minősülhet.

A 32. cikk egyértelműen megfogalmazza, hogy az adatkezelőnek és az adatfeldolgozónak megfelelő technikai és szervezési intézkedéseket kell hoznia a személyes adatok megfelelő szintű biztonságának garantálása érdekében: az incidensek időben történő észlelése, kezelése és jelentése iránti képességnek ezen intézkedések alapvető elemét kell képeznie.

3. Közös adatkezelők

A 26. cikk a közös adatkezelőkkel foglalkozik, és rögzíti, hogy a közös adatkezelőknek meg kell határozniuk az általános adatvédelmi rendelet betartásáért fennálló felelősségük megoszlását[25]. Ennek keretében ki kell jelölniük azt a felet, aki a 33. és 34. cikkben foglalt kötelezettségek teljesítéséért felel. A 29. cikk szerinti munkacsoport azt ajánlja, hogy a közös adatkezelők közötti szerződéses megállapodás tartalmazzon rendelkezéseket arra vonatkozóan, melyik adatkezelőé lesz a vezető szerep vagy a felelősség az általános adatvédelmi rendelet incidensbejelentési kötelezettségeinek teljesítésével összefüggésben.

4. Az adatfeldolgozó kötelezettségei

A személyes adatok védelme iránti általános felelősség megmarad az adatkezelőnél, de az adatfeldolgozónak is lényeges szerepe van abban, hogy az adatkezelő eleget tudjon tenni a kötelezettségeinek, köztük az adatvédelmi incidens bejelentésének. Sőt, a 28. cikk (3) bekezdése előírja, hogy az adatfeldolgozó által végzett adatkezelést szerződésnek vagy más jogi aktusnak kell szabályoznia. A 28. cikk (3) bekezdésének f) pontja szerint a szerződésnek vagy más jogi aktusnak rendelkeznie kell arról, hogy az adatfeldolgozó „segíti az adatkezelőt a 32–36. cikk szerinti kötelezettségek teljesítésében, figyelembe véve az adatkezelés jellegét és az adatfeldolgozó rendelkezésére álló információkat”.

A 33. cikk (2) bekezdése egyértelműen kimondja, hogy amennyiben az adatkezelő adatfeldolgozót vesz igénybe, és az adatfeldolgozó az adatkezelő nevében általa kezelt személyes adatokat érintő adatvédelmi incidensről szerez tudomást, akkor azt „indokolatlan késedelem nélkül” be kell jelentenie az adatkezelőnek. Megjegyzendő, hogy az adatfeldolgozónak nem szükséges felmérnie az incidensből eredő kockázat valószínűségét, mielőtt bejelentést tesz az adatkezelőnek; ezt az adatkezelőnek kell felmérnie, miután tudomására jut az incidens. Az adatkezelőnek mindössze azt kell megállapítania, hogy történt-e incidens, ezt követően pedig értesítenie kell az adatkezelőt. Az adatkezelő a céljai eléréséhez veszi igénybe az adatfeldolgozót, ezért elvben akkor tekinthető úgy, hogy az adatkezelő tudomására jutott az incidens, amikor az adatfeldolgozó tájékoztatta róla. Az adatkezelő értesítésére vonatkozó adatfeldolgozói kötelezettség révén nyílik lehetősége az adatkezelőnek, hogy kezelje az incidenst, és megállapítsa, hogy szükséges-e a 33. cikk (1) bekezdése szerint bejelentést tenni a

[24] Lásd az időtartamokra, időpontokra és határidőkre vonatkozó szabályok meghatározásáról szóló 1182/71/EGK, Euratom rendeletet, amely a következő internetcímen érhető el: https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:31971R1182&from=HU

[25] Lásd még a (79) preambulumbekezdést.

felügyeleti hatóságnak, a 34. cikk (1) bekezdése értelmében pedig értesíteni az érintetteket. Előfordulhat, hogy az adatkezelő egyúttal ki kívánja vizsgálni az incidenst, mivel az adatfeldolgozó nincs feltétlenül abban a helyzetben, hogy az üggyel kapcsolatos összes lényeges tényt ismerje, például akkor, ha az adatfeldolgozó által megsemmisített vagy elveszített személyes adatok példánya vagy biztonsági másolata még az adatkezelő birtokában van. Ez befolyásolhatja, hogy az adatkezelőnek ezt követően kell-e bejelentést tennie.

Az általános adatvédelmi rendelet nem határoz meg kifejezett határidőt, amelyen belül az adatfeldolgozónak figyelmeztetnie kell az adatkezelőt, mindössze azt írja elő, hogy ezt „indokolatlan késedelem nélkül" kell megtennie. A 29. cikk szerinti munkacsoport ezért azt ajánlja, hogy az adatfeldolgozó haladéktalanul értesítse az adatkezelőt, további tájékoztatást pedig nyújthat részletekben, amikor több adat áll a rendelkezésére. Ez azért fontos, mivel ezzel segíthet az adatkezelőnek teljesíteni a felügyeleti hatóságnak 72 órán belül való bejelentésre vonatkozó követelményt.

Az adatkezelő és az adatfeldolgozó közötti szerződésben a fent leírtak szerint meg kell határozni, hogyan kell eleget tenni az általános adatvédelmi rendelet más rendelkezésein túlmenően a 33. cikk (2) bekezdésében rögzített követelményeknek. E körbe tartozhat az adatkezelő általi gyors bejelentésre vonatkozó követelmény, amelynek betartása esetén az adatkezelő pedig könnyebben teljesíteni tudja a felügyeleti hatóságnak 72 órán belül való bejelentésre vonatkozó kötelezettségeit.

Ha az adatfeldolgozó egyszerre több adatkezelőnek nyújt szolgáltatást, és ugyanaz az incidens az összes ilyen adatkezelőt érinti, az adatfeldolgozónak mindegyik adatkezelő számára jelentenie kell az incidens részleteit.

Az adatfeldolgozó bejelentést tehet az adatkezelő nevében, amennyiben erre megfelelő meghatalmazást kapott az adatkezelőtől, és ez az adatkezelő és az adatfeldolgozó közötti szerződéses megállapodás részét képezi. Ezt a bejelentést a 33. és 34. cikknek megfelelően kell megtenni. Azt azonban fontos megjegyezni, hogy a bejelentés iránti jogi felelősség változatlanul az adatkezelőt terheli.

B. A felügyeleti hatóság tájékoztatása

1. A közlendő információk köre

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

> „a) ismertetni kell az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát;
>
> b) közölni kell az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;
>
> c) ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket;
>
> d) ismertetni kell az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket."

Az általános adatvédelmi rendelet nem határozza meg az érintettek vagy a személyes adatok kategóriáit. A 29. cikk szerinti munkacsoport mindazonáltal az érintett olyan kategóriáinak meghatározását javasolja, amelyek megfelelnek azon egyének különböző típusainak, akinek a személyes adatait az incidens érintette: az alkalmazott leíró jellemzőktől függően ilyen kategóriákat

alkothatnak többek között a gyermekek és más veszélyeztetett csoportok, a fogyatékossággal élők, a munkavállalók és az ügyfelek. A személyes adatok kategóriái hasonlóképpen megfeleltethetők az adatkezelő által kezelt adatok különböző típusainak, így egyebek mellett lehetnek egészségügyi adatok, oktatási nyilvántartások, szociális ellátási információk, pénzügyi adatok, bankszámlaszámok és útlevélszámok.

A (85) preambulumbekezdés egyértelműen megfogalmazza, hogy a bejelentés egyik célja az egyéneket érő kár korlátozása. Ennek megfelelően akkor, ha az érintettek vagy a személyes adatok jellege arra enged következtetni, hogy fennáll az incidens eredményeként bekövetkező kár (például személyazonosság-lopás, csalás, pénzügyi veszteség, a szakmai titoktartás veszélybe kerülése) kockázata, akkor fontos, hogy a bejelentés tartalmazza ezeket a kategóriákat. Ily módon összefügg az incidensből eredő, valószínűsíthető következmények ismertetésére vonatkozó követelménnyel.

Az incidens időben történő bejelentése előtt az sem lehet akadály, ha nem állnak rendelkezésre pontos információk (például az érintettek pontos száma). Az általános adatvédelmi rendelet megengedi az érintett személyek és személyes adatok számának hozzávetőleges megadását. A hangsúlyt nem a pontos számadatok közlésére, hanem az incidens hátrányos hatásainak kezelésére kell fektetni. Így amikor egyértelművé válik, hogy incidens történt, de annak terjedelme még nem ismert, akkor a részletekben történő bejelentés (lásd lent) biztos módja lehet a bejelentési kötelezettségek teljesítésének.

A 33. cikk (3) bekezdése kimondja, hogy az adatkezelőnek „legalább” a megjelölt információkat kell közölnie a bejelentésben, tehát szükség szerint dönthet úgy, hogy további részleteket ad meg. Előfordulhat, hogy eltérő jellegű incidensek (titoksértés, sértetlenségi adatsértés vagy hozzáférhetőségi adatsértés) előfordulása estén további információkkal kell szolgálni mindegyik eset körülményeinek maradéktalan ismertetéséhez.

Példa

Az adatkezelő hasznosnak találhatja a felügyeleti hatóságnak tett bejelentésében megnevezni az általa igénybe vett adatfeldolgozót, amennyiben az adatvédelmi incidens az adatfeldolgozóra vezethető vissza, különösen akkor, ha az ugyanazon adatfeldolgozót igénybe vevő számos másik adatkezelő birtokában lévő személyes adatokat érintő incidenst okozott.

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

2. Bejelentés részletekben

Az incidens jellegétől függően előfordulhat, hogy az adatkezelőnek további vizsgálatot kell lefolytatnia az incidens szempontjából lényeges összes tény megállapítása céljából. A 33. cikk (4) bekezdése ezért a következőképpen rendelkezik:

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

Az általános adatvédelmi rendelet tehát elismeri, hogy az adatkezelők nem mindig rendelkeznek az incidensről való tudomásszerzéstől számított 72 órán belül az összes szükséges információval, ugyanis nem minden esetben állnak rendelkezésre maradéktalan és minden részletre kiterjedő adatok az incidensről ebben a kezdeti időszakban. A rendelet ezért megengedi a részletekben történő bejelentést. Valószínűleg gyakrabban fordul majd el a bonyolultabb incidensek, így bizonyos fajta kiberbiztonsági incidensek esetében, amikor például mélyreható kriminalisztikai vizsgálatra lehet szükség az incidens jellegének és a veszélybe került személyes adatok körének pontos megállapításához. Következésképpen az adatkezelőnek sok esetben további vizsgálatokat kell

végrehajtania, hogy később kiegészítő információkkal tudjon szolgálni. Ez megengedhető abban az esetben, ha az adatkezelő a 33. cikk (1) bekezdésében foglaltak szerint megindokolja a késedelmet. A 29. cikk szerinti munkacsoport azt ajánlja, hogy amikor az adatkezelő első alkalommal tesz bejelentést a felügyeleti hatóságnak, mindig tájékoztatnia kell a hatóságot arról, ha még nem rendelkezik az összes szükséges információval, és a későbbiekben fog további részleteket közölni. A felügyeleti hatóságnak el kell fogadnia a kiegészítő információk közlésének módját és idejét. Az adatkezelő ettől függetlenül kiegészítő információkkal szolgálhat bármilyen más időpontban vagy akkor, amikor olyan további lényeges adatok jutnak a tudomására, amelyeket közölnie kell a felügyeleti hatósággal.

A bejelentési követelmény elsődleges célja, hogy arra ösztönözze az adatkezelőket, hogy incidens felmerülése esetén haladéktalanul intézkedjenek, hárítsák el azt, és lehetőség szerint állítsák helyre a veszélybe került személyes adatokat, valamint ezzel összefüggésben kérjenek tanácsot a felügyeleti hatóságtól. Ha 72 órán belül bejelentést tesz a felügyeleti hatóságnak, az adatkezelő megbizonyosodhat arról, hogy helyesen döntött-e az egyének értesítéséről vagy annak mellőzéséről.

A felügyeleti hatóságnak tett bejelentés célja azonban nem kizárólag az, hogy az adatkezelők tanácsot kapjanak azzal kapcsolatosan, hogy értesíteniük kell-e az érintett egyéneket. Bizonyos esetekben az incidens jellege és a kockázat súlyossága miatt egyértelmű lesz, hogy az adatkezelőnek haladéktalanul értesítenie kell az érintett egyéneket. Ha például fennáll a személyazonosság-lopás közvetlen fenyegetése, vagy különleges kategóriájú személyes adatok[26] kerülnek nyilvánosságra az interneten, az adatkezelőnek indokolatlan késedelem nélkül intézkednie kell az incidens elhárításáról és az érintett egyének tájékoztatásáról (lásd a III. szakaszt). Kivételes körülmények között erre még a felügyeleti hatóságnak való bejelentés megtétele előtt sor kerülhet. Általánosabban fogalmazva a felügyeleti hatóságnak való bejelentés nem indokolhatja az érintettek incidensről való tájékoztatásának elmulasztását abban az esetben, amikor kötelező ilyen tájékoztatást nyújtani.

Leszögezendő még, hogy az adatkezelő az első bejelentést követően naprakész tájékoztatást nyújthat a felügyeleti hatóságnak, ha további vizsgálat során olyan tényekre derül fény, amelyek alátámasztják, hogy a biztonsági incidenst elhárították, és valójában nem történt adatvédelmi incidens. Ezekkel az információkkal ezután kiegészíthető a felügyeleti hatóságnak addig nyújtott tájékoztatás, az incidens nyilvántartásba vételekor pedig rögzíthető, hogy nem adatvédelmi incidens történt. Semmilyen szankció nem jár olyan incidens bejelentéséért, amelyről végül kitudódik, hogy nem adatvédelmi incidens volt.

Példa

Egy adatkezelő az adatvédelmi incidens észlelésétől számított 72 órán belüli bejelentést tesz a felügyeleti hatóságnak arról, hogy elveszítette az egyes ügyfelei személyes adatainak másolatát tartalmazó USB-kulcsot. Később kiderül, hogy az USB-kulcsot rossz helyre tették az adatkezelő helyiségein belül, így végül megkerül. Az adatkezelő tájékoztatja a felügyeleti hatóságot, és a bejelentés módosítását kéri.

Megjegyzendő, hogy a részletekben történő bejelentésre a 2002/58/EK irányelvben és a 611/2013/EU rendeletben foglalt kötelezettségek és más, önállóan bejelentett incidensek esetében már eddig is volt lehetőség.

3. Késedelmes bejelentés

A 33. cikk (1) bekezdése egyértelművé teszi, hogy ha a bejelentés nem történik meg 72 órán belül, mellékelni kell hozzá a késedelem igazolására szolgáló indokokat is. Ez a szakaszokban történő

[26] Lásd a 9. cikket.

bejelentés elgondolásával együtt annak elismerése, hogy az adatkezelő nem minden esetben tudja bejelenteni az incidenst a megadott időn belül, így megengedhető a késedelmes bejelentés.

Ez a helyzet például akkor fordulhat elő, ha az adatkezelő rövid időn belül több hasonló titoksértést észlel, amely nagyszámú érintettre gyakorol ugyanolyan hatást. Az adatkezelő tudomást szerezhet egy incidensről, és annak kivizsgálásának megkezdésekor, a bejelentést megelőzően további hasonló incidenseket észlelhet, amelyek eltérő okból merülnek fel. A körülményektől függően némi időbe telhet, amíg az adatkezelő megállapítja az incidensek terjedelmét, és ahelyett, hogy mindegyiket külön jelentené be, összeállíthat egy jelentőségteljesebb bejelentést több, eltérő okból bekövetkezett, de nagyon hasonló incidensről. Ennek következtében előfordulhat, hogy a felügyeleti hatóságnak való bejelentés megtétele több mint 72 órát vesz igénybe attól számítva, amikor az adatkezelő tudomást szerzett az incidensekről.

Szigorúan véve minden egyes adatvédelmi incidens bejelentendő. Azonban a túlzott terhelés elkerülése érdekében az adatkezelő benyújthat az összes incidensre vonatkozó, „összevont" bejelentést, feltéve, ha az incidensek viszonylag rövid időn belül ugyanolyan módon megsértett, azonos jellegű személyes adatokat érintenek. Ha sorozatosan következnek be olyan incidensek, amelyek különböző módon megsértett, eltérő jellegű személyes adatokat érintenek, akkor a bejelentést a szokott módon kell megtenni, tehát mindegyik incidenst a 33. cikk szerint kell jelenteni.

Míg az általános adatvédelmi rendelet bizonyos fokig megengedi a késedelmes bejelentést, ez azonban nem válthat rendszeressé. Érdemes kiemelni, hogy összevont bejelentést több hasonló, 72 órán belül jelentett incidensről is lehet tenni.

C. Több országot érintő incidensek és Unión kívüli tevékenységi helyen bekövetkező incidensek

1. Több országot érintő incidensek

Személyes adatok határokon átnyúló kezelése[27] esetén az incidens több tagállamban is kihatással lehet érintettekre. A 33. cikk (1) bekezdése egyértelműen fogalmaz a tekintetben, hogy amennyiben incidens történik, az adatkezelőnek bejelentést kell tennie az általános adatvédelmi rendelet 55. cikke szerint illetékes felügyeleti hatóságnak[28]. Az 55. cikk (1) bekezdése a következőképpen rendelkezik:

> „A felügyeleti hatóság a saját tagállamának területén illetékes az e rendelet alapján ráruházott feladatok végzésére és hatáskörök gyakorlására."

Ugyanakkor az 56. cikk (1) bekezdése az alábbiakat mondja ki:

> „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."

Ezen túlmenően az 56. cikk (6) bekezdése így rendelkezik:

> „A fő felügyeleti hatóság az adatkezelő vagy adatfeldolgozó egyetlen kapcsolattartója az általuk végzett, határokon átnyúló adatkezeléssel kapcsolatban."

[27] Lásd a 4. cikk (23) bekezdését

[28] Lásd még a (122) preambulumbekezdést.

Ennek értelmében akkor, amikor az incidens határokon átnyúló adatkezeléssel összegfüggésben merül fel, és kötelező bejelenteni, az adatkezelőnek a fő felügyeleti hatóságnak[29] kell bejelentést tennie. Ezért az incidenskezelési terv kidolgozása során az adatkezelőnek meg kell vizsgálnia, melyik felügyeleti hatóság a fő felügyeleti hatóság, amelynek bejelentést kell majd tennie[30]. Az adatkezelő ezáltal azonnal reagálhat az incidensekre, és teljesítheti a 33. cikk tekintetében fennálló kötelezettségeit. Világosan kell tehát látni, hogy határokon átnyúló adatkezelést érintő incidens esetén a fő felügyeleti hatóságnak kell bejelentést tenni, ez a hatóság azonban nem feltétlenül ugyanott működik, ahol az érintettek találhatók, vagy akár az incidens történt. A fő hatóság értesítésekor az adatkezelőnek adott esetben jeleznie kell, hogy az incidens más tagállamokban található tevékenységi helyeket érint, és valószínűsíthetően mely tagállamokban van hatással az incidens érintettekre. Ha az adatkezelőnek kétségei vannak a fő felügyeleti hatóság kilétét illetően, akkor legalább azon ország felügyeleti hatóságának bejelentést kell tennie, ahol az incidens történt.

2. Unión kívüli tevékenységi helyen bekövetkező incidensek

Az általános adatvédelmi rendelet területi hatályáról a 3. cikk rendelkezik, és egyebek mellett azt is meghatározza, hogy a rendelet mikor alkalmazandó a személyes adatoknak a nem az Unióban tevékenységi hellyel rendelkező adatkezelő vagy adatfeldolgozó által végzett kezelésére. Ezzel összefüggésben kiemelendő a 3. cikk (2) bekezdése[31]:

> „E rendeletet kell alkalmazni az Unióban tartózkodó érintettek személyes adatainak az Unióban tevékenységi hellyel nem rendelkező adatkezelő vagy adatfeldolgozó által végzett kezelésére, ha az adatkezelési tevékenységek:
>
> a) áruknak vagy szolgáltatásoknak az Unióban tartózkodó érintettek számára történő nyújtásához kapcsolódnak, függetlenül attól, hogy az érintettnek fizetnie kell-e azokért; vagy
>
> b) az érintettek viselkedésének megfigyeléséhez kapcsolódnak, feltéve hogy az Unió területén belül tanúsított viselkedésükről van szó.”

Lényeges a 3. cikk (3) bekezdése is, amely így rendelkezik[32]:

> „E rendeletet kell alkalmazni a személyes adatoknak a nem az Unióban, hanem olyan helyen tevékenységi hellyel rendelkező adatkezelő által végzett kezelésére, ahol a nemzetközi közjog értelmében valamely tagállam joga alkalmazandó.”

Amennyiben az Unióban tevékenységi hellyel nem rendelkező adatkezelő a 3. cikk (2) vagy (3) bekezdése hatálya alá tartozik, és incidenst észlel, akkor ez esetben rá is vonatkoznak a 33. és a 34. cikkben rögzített bejelentési kötelezettségek. A 27. cikk előírja, hogy az adatkezelő (és az adatfeldolgozó) a 3. cikk (2) bekezdésében meghatározott esetben jelöljön ki uniós képviselőt. Ilyen esetben a 29. cikk szerinti munkacsoport azt ajánlja, hogy azon tagállam felügyeleti hatóságának tegyenek bejelentést, ahol az adatkezelő uniós képviselője tevékenységi hellyel, illetve lakóhellyel

---

[29] Lásd a 29. cikk szerinti munkacsoportnak az adatkezelő vagy az adatfeldolgozó fő felügyeleti hatóságának meghatározásáról szóló iránymutatását, amely a következő internetcímen érhető el: http://ec.europa.eu/newsroom/document.cfm?doc_id=44102

[30] Az Európa összes nemzeti adatvédelmi hatóságának elérhetőségeit tartalmazó jegyzék a következő internetcímen érhető el: http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm

[31] Lásd még a (23) és a (24) preambulumbekezdést.

[32] Lásd még a (25) preambulumbekezdést.

rendelkezik[33]. Ehhez hasonlóan akkor, ha az adatfeldolgozó a 3. cikk (2) bekezdésének hatálya alá tartozik, az adatfeldolgozókat terhelő kötelezettségek vonatkoznak rá, amelyek közül ez esetben különösen az adatkezelő incidensről való értesítését illetően a 33. cikk (2) bekezdésében rögzített kötelezettség lényeges.

D. A bejelentés mellőzésének feltételei

A 33. cikk (1) bekezdése egyértelműen rögzíti, hogy nem szükséges bejelenteni a felügyeleti hatóságnak azt az incidenst, amely „valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve". Példaként felhozható az az eset, amikor a személyes adatok már nyilvánosan hozzáférhetőek, és az ilyen adatok közlése valószínűleg nem jelent kockázatot az egyén számára. Ez ellentétben áll azokkal a nyilvánosan elérhető elektronikus hírközlési szolgáltatást nyújtó szolgáltatók számára a 2009/136/EK irányelvben előírt incidensbejelentési követelményekkel, amelyek szerint minden vonatkozó incidenst jelenteni kell az illetékes hatóságnak.

A személyes adatok megsértése bejelentéséről szóló 03/2014 sz. véleményében[34] a 29. cikk szerinti munkacsoport kifejtette, hogy a legkorszerűbb algoritmussal titkosított személyes adatok titkosságának megsértése is adatvédelmi incidensnek minősül, így bejelentendő. Ha azonban a kulcs titkossága sértetlen (vagyis a kulcsot nem veszélyeztette a biztonságnak semmilyen megsértése, és úgy került generálásra, hogy az elérhető technológiai eszközökkel senki olyan nem derítheti ki, aki a kulcshoz nem jogosult hozzáférni), akkor az adatok elvben értelmezhetetlenek. Így nem valószínű, hogy az incidens hátrányos hatást gyakorolna egyénekre, ezért nem szükséges őket tájékoztatni[35]. Ám amennyiben az adatok titkosítottak, a veszteség vagy módosítás hátrányos következményekkel járhat az érintettekre, ha az adatkezelőnek nincsenek megfelelő biztonsági másolatai. Ebben az esetben még akkor is szükséges az érintettek tájékoztatása, ha magukat az adatokat megfelelően titkosították.

A 29. cikk szerinti munkacsoport azt is kifejtette, hogy akkor is hasonló a helyzet, ha a személyes adatokat – például a jelszavakat – biztonságosan hasították és kiegészítő jelszavazták, a hasított értéket magas szintű kriptográfiai kulcsos szabványos hasítófüggvénnyel számolták ki, az adatok hasítására használt kulcsot nem veszélyeztette a biztonságnak semmilyen megsértése, és az adatok hasításához használt kulcsot úgy generálták, hogy az elérhető technológiai eszközökkel azt senki olyan nem derítheti ki, aki a kulcshoz nem jogosult hozzáférni.

Következésképpen akkor, ha a személyes adatokat jogosulatlan felek számára lényegében értelmezhetetlenné tették, és létezik belőlük még egy példány vagy biztonsági másolat, a megfelelően titkosított személyes adatok titkosságának megsértését nem feltétlenül szükséges bejelenteni a felügyeleti hatóságnak. Ennek oka, hogy az ilyen incidens valószínűsíthetően nem jár kockázattal az egyének jogaira és szabadságaira nézve. Ez természetesen azt jelenti, hogy az egyéneket sem kell tájékoztatni, mivel feltehetőleg nem merül fel jelentős kockázat. Ugyanakkor szem előtt kell tartani, hogy kezdetben talán nem szükséges bejelentést tenni, ha valószínűsíthetően nincs az egyének jogait és szabadságait érintő kockázat, ez azonban idővel változhat, és előfordulhat, hogy újra fel kell mérni a kockázatot. Ha például utólag kiderül a kulcsról, hogy veszélybe került, vagy sebezhetőségre derül fény a titkosító szoftverben akkor szükség lehet bejelentésre.

Ezenkívül megjegyzendő, hogy ha olyan esetben fordul elő incidens, amikor a titkosított személyes adatokról nincsenek biztonsági másolatok, akkor hozzáférhetőségi adatsértés történik, amely

[33] Lásd a (80) preambulumbekezdést és a 27. cikket.

[34] A 29. cikk szerinti munkacsoport, 03/2014 sz. vélemény a személyes adatok megsértése bejelentéséről, http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp213_hu.pdf

[35] Lásd még a 611/2013/EU rendelet 4. cikkének (1) és (2) bekezdését.

kockázatokkal járhat az egyénekre nézve, ezért be kell jelenteni. Hasonló a helyzet a titkosított adatok elvesztésével járó incidens esetén: még ha van is biztonsági másolat a személyes adatokról, akkor is előfordulhat, hogy jelentendő az incidens, attól függően, mennyi időt vesz igénybe az adatok helyreállítása a biztonsági másolatból, és milyen kihatással van a hozzáférhetetlenség az egyénekre. Ahogy a 32. cikk (1) bekezdésének c) pontja is rögzíti, a biztonság fontos tényezőjének kell tekinteni „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".

Példa

A felügyeleti hatóságnak való bejelentést nem igénylő incidens lehet az adatkezelő és alkalmazottai által használt, biztonságosan titkosított mobilkészülék elvesztése. Amennyiben a titkosítási kulcs biztonságosan továbbra is az adatkezelő birtokában van, és nem a készüléken volt a személyes adatok egyetlen példánya, akkor ezekhez az adatokhoz semmilyen támadó nem tud hozzáférni. Következésképpen az incidens valószínűsíthetően nem jár kockázattal a kérdéses érintettek jogaira és szabadságaira nézve. Ha később nyilvánvalóvá válik, hogy a titkosítási kulcs veszélybe került, illetve a titkosító szoftver vagy algoritmus sebezhető, akkor a természetes személyek jogait és szabadságait érintő kockázat megváltozik, így már szükség lehet bejelentésre.

Azonban a 33. cikkben foglaltak be nem tartása merül fel, ha az adatkezelő nem tesz bejelentést a felügyeleti hatóságnak olyan helyzetben, amikor az adatok valójában nem voltak biztonságosan titkosítva. Ezért a titkosító szoftver kiválasztásakor az adatkezelőknek gondosan mérlegelniük kell a kínált titkosítás minőségét és megfelelő végrehajthatóságát, valamint tisztában kell lenniük azzal, hogy ténylegesen milyen mértékű védelmet biztosít, és ez arányban van-e a felmerülő kockázatokkal. Az adatkezelőknek emellett részletekbe menően ismerniük kell a titkosító termék működését. Például előfordulhat, hogy valamely készülék titkosítható kikapcsolás után, de nem készenléti üzemmódban. A titkosítást alkalmazó termékek egy része „alapértelmezett kulcsot" használ, amelyet a hatékonyság érdekében mindegyik ügyfélnek módosítania kell. Emellett előfordulhat, hogy biztonsági szakértők az adott időpontban megfelelőnek ítélik a titkosítást, azonban néhány éven belül elavulttá válhat, ezzel pedig kérdésessé válhat, hogy az adott termék kellőképpen titkosítja az adatokat, és megfelelő mértékű védelmet nyújt-e.

III. 34. cikk – Az érintett tájékoztatása

A. Egyének tájékoztatása

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

A 34. cikk (1) bekezdése szerint:

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

Emlékeztetjük az adatkezelőket, hogy kötelező bejelentést tenni a felügyeleti hatóságnak, kivéve, ha az incidens valószínűsíthetően nem jár kockázattal az egyének jogaira és szabadságaira nézve. Ezenkívül abban az esetben, ha az incidens valószínűsíthetően jelentős kockázattal jár az egyének jogaira és szabadságaira nézve, tájékoztatni kell az egyéneket. Az egyének incidensről való tájékoztatására vonatkozó küszöb tehát magasabb, mint a felügyeleti hatóságoknak való bejelentés esetében, ezért nem szükséges minden incidensről tájékoztatni az egyéneket, ezzel megkímélve őket attól, hogy a szükségtelen értesítések miatt közömbössé váljanak.

Az általános adatvédelmi rendelet kimondja, hogy az egyéneket „indokolatlan késedelem nélkül”, vagyis a lehető leghamarabb tájékoztatni kell az incidensről. Az egyének értesítésének elsődleges célja, hogy konkrét tájékoztatást kapjanak arról, milyen intézkedésekkel gondoskodhatnak a saját védelmükről[36]. Ahogyan a fentiekben már kifejtettük, ha az incidens jellegétől és a felmerülő kockázattól függően időben tájékoztatást kapnak, az egyének könnyebben intézkedhetnek az incidens esetleges hátrányos következményei elleni védelmükről.

Ezen iránymutatás B. melléklete a teljesség igénye nélkül példákat sorol fel arra vonatkozóan, mikor járnak az incidensek valószínűsíthetően jelentős kockázattal az egyének számára, következésképpen melyek azok az esetek, amikor az adatkezelőnek értesítenie kell az érintetteket az incidensről.

B. A közlendő információk köre

Az egyének értesítését illetően a 34. cikk (2) bekezdése a következőképpen rendelkezik:

> „Az (1) bekezdésben említett, az érintett részére adott tájékoztatásban világosan és közérthetően ismertetni kell az adatvédelmi incidens jellegét, és közölni kell legalább a 33. cikk (3) bekezdésének b), c) és d) pontjában említett információkat és intézkedéseket.”

E rendelkezés értelmében az adatkezelőnek legalább az alábbi tájékoztatást kell nyújtania:

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

Az incidens orvoslására és az esetleges hátrányos következmények enyhítésére tett intézkedés lehet például, ha az adatkezelő az incidens illetékes felügyeleti hatóságnak való bejelentését követően jelezheti, hogy tanácsot kapott az incidens kezelésére és hatásának mérséklésére vonatkozóan. Az adatkezelő emellett adott esetben konkrét tanácsokkal láthatja el az egyéneket, hogy védekezni tudjanak az incidens esetleges hátrányos következményeivel szemben, például javasolhatja, hogy állítsanak be maguknak új jelszót, amennyiben hozzáférési hitelesítő adataik kerültek veszélybe. Az adatkezelő ez esetben is dönthet úgy, hogy az itt előírtaknál bővebb tájékoztatást nyújt.

C. Kapcsolatfelvétel az egyénekkel

Az érintetteket elvben közvetlenül kell tájékoztatni az adott incidensről, kivéve, ha ez aránytalan erőfeszítéssel járna. Ilyen esetekben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, vagy olyan hasonló intézkedést kell hozni, amely biztosítja az érintettek hasonlóan hatékony tájékoztatását (a 34. cikk (3) bekezdésének c) pontja).

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

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

[36] Lásd még a (86) preambulumbekezdést.

sajtóközleményre vagy vállalati blogbejegyzésre korlátozódó értesítéssel nem lehet hatékonyan tájékoztatni az egyéneket az incidensről. A 29. cikk szerinti munkacsoport azt ajánlja az adatkezelőknek, hogy olyan megoldást válasszanak, amellyel a legnagyobb az esély arra, hogy minden érintett egyént megfelelően tájékoztatnak. A körülményektől függően elképzelhető, hogy az adatkezelőnek többféle tájékoztatási eszközt is igénybe kell vennie, ahelyett, hogy egyetlen kapcsolattartási csatornára hagyatkozna.

Előfordulhat, hogy az adatkezelőnek arról is gondoskodnia kell, hogy a tájékoztatás megfelelő alternatív formákban és a lényeges nyelveken is hozzáférhető legyen, hogy az egyének megértsék a velük közölt információkat. Például az egyének incidensről való tájékoztatásakor általában véve helyénvaló azt a nyelvet használni, amelyen korábban a rendes üzletmenet során a címzettel kommunikáltak. Ha azonban az incidens olyan érintettekre van kihatással, akikkel az adatkezelőnek addig nem volt kapcsolata, a szükséges források figyelembevétele mellett elfogadható lehet a helyi hivatalos nyelv használata, különösen akkor, ha az ilyen érintettek az adatkezelő tevékenységi helyétől eltérő tagállamban vagy egyéb, nem uniós országban rendelkeznek lakóhellyel. A lényeg, hogy segíteni kell az érintetteknek az incidens jellegének és a saját védelmük érdekében tehető intézkedéseknek a megértésében.

Az adatkezelőknek érdemes az egyének incidensről való tájékoztatására legalkalmasabb kapcsolattartási csatornát kiválasztaniuk, különösen akkor, ha gyakran lépnek kapcsolatban az ügyfeleikkel. Ugyanakkor egyértelmű, hogy az adatkezelőnek tartózkodnia kell az incidens által veszélyeztetett kapcsolattartási csatorna használatától, mivel előfordulhat, hogy a támadók ezen a csatornán keresztül az adatkezelőnek adják ki magukat.

A (86) preambulumbekezdés egyúttal az alábbiakat is rögzíti:

> „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. Például az érintettek sürgős tájékoztatása a kár közvetlen veszélyének mérsékléséhez szükséges, azonban annak megelőzése több időt igényelhet, hogy a folyamatos vagy azonos jellegű adatvédelmi incidens esetében megfelelő intézkedéseket kell végrehajtani.”

Az adatkezelőknek tehát azért érdemes kapcsolatba lépniük és egyeztetniük a felügyeleti hatósággal, hogy tanácsot kérjenek nemcsak az érintetteknek a 34. cikk értelmében az incidensről való tájékoztatásáról, hanem az egyéneknek küldendő megfelelő üzenetekről és a legalkalmasabb kapcsolatfelvételi módról is.

Ehhez kapcsolódik a (88) preambulumbekezdésben megfogalmazott tanács, miszerint az incidensről való értesítés során figyelembe kell venni „a bűnüldöző hatóságok jogos érdekeit olyan esetekben, amikor az idő előtti közlés szükségtelenül veszélyeztethetné az adatvédelmi incidens körülményeinek kivizsgálását”. Ez úgy értelmezhető, hogy amennyiben indokolt, az adatkezelő bizonyos körülmények között, a bűnüldöző hatóságok tanácsára késleltethetik az érintett egyének incidensről való tájékoztatását mindaddig, amíg ez hátrányosan befolyásolhatja a kivizsgálást. Ezt követően azonban haladéktalanul tájékoztatni kell az érintetteket.

Amennyiben az adatkezelőnek azért nem áll módjában tájékoztatni valamely egyént, mivel nem rendelkezik elegendő adattal a kapcsolatfelvételhez, e sajátos körülményre tekintette tájékoztathatja az egyént akkor, amikor ez észszerűen megvalósítható (például akkor, amikor az egyén gyakorolja a 15. cikkben rögzített jogát, hogy hozzáférjen a személyes adataihoz, és megadja az adatkezelőnek a kapcsolatfelvételhez szükséges kiegészítő adatokat).

D. A tájékoztatás mellőzésének feltételei

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

- az adatkezelő az incidens bekövetkezése előtt megfelelő technikai és szervezési intézkedéseket alkalmazott személyes adatok védelme érdekében, ideértve különösen azokat az intézkedéseket, amelyek a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik az adatokat. Ilyen intézkedés lehet például a személyes adatok legkorszerűbb titkosítással vagy jogkivonat-létrehozással történő védelme;
- az adatkezelő rögtön az incidenst követően intézkedéseket tett annak biztosítása érdekében, hogy az egyének jogaira és szabadságaira jelentett magas kockázat a továbbiakban valószínűsíthetően ne valósuljon meg. Az eset körülményeitől függően például előfordulhat, hogy az adatkezelő azonnal azonosította azt az egyént, aki még azelőtt hozzáfért a személyes adatokhoz, mielőtt bármit lehetett volna velük kezdeni, és intézkedéseket hozhatott vele szemben. Ekkor is kellő figyelmet kell fordítani a titoksértés lehetséges következményeire, szintén az érintett adatok jellegétől függően;
- az egyénekkel való kapcsolatfelvétel aránytalan erőfeszítést tenne szükségessé[37], talán azért, mert elérhetőségi adataik az incidens következtében elvesztek, vagy eleve nem is voltak ismertek. Például a statisztikai hivatal raktárát elönti a víz, és a személyes adatokat tartalmazó dokumentumokat kizárólag papíralapon tárolták. Az adatkezelőnek ilyenkor nyilvánosan közzétett információk útján kell tájékoztatnia az egyéneket, vagy olyan hasonló intézkedést kell hoznia, amely biztosítja a hasonlóan hatékony tájékoztatásukat. Amennyiben aránytalan erőfeszítésre lenne szükség, olyan technikai megoldások is alkalmazhatók, amelyekkel igény szerint válik hozzáférhetővé az incidenssel kapcsolatos tájékoztatás. Ez azoknál az egyéneknél bizonyulhat hasznosnak, akiket az incidens érintett, de az adatkezelő nem tud más módon kapcsolatba lépni velük.

Az elszámoltathatósági elvnek megfelelően az adatkezelőknek tudniuk kell bizonyítani a felügyeleti hatóság felé, hogy e feltételek közül egynek vagy többnek megfelelnek [38]. Szem előtt kell tartani, hogy kezdetben talán nem szükséges bejelentést tenni, ha nincs a természetes személyek jogait és szabadságait érintő kockázat, ez azonban idővel változhat, és előfordulhat, hogy újra fel kell mérni a kockázatot.

Amennyiben az adatkezelő úgy dönt, hogy nem tájékoztatja az egyént az incidensről, a felügyeleti hatóság a 34. cikk (4) bekezdése értelmében kötelezheti erre, ha úgy véli, hogy az incidens valószínűsíthetően magas kockázattal jár az egyének számára. Ellenkező esetben megítélheti úgy, hogy a 34. cikk (3) bekezdésében rögzített feltételek teljesülnek, így nem szükséges értesíteni az egyéneket. Ha a felügyeleti hatóság megállapítja, hogy az érintettek értesítésének mellőzésére vonatkozó döntés nem megalapozott, akkor élhet a rendelkezésére álló hatáskörrel és szankciókkal.

IV. A kockázat és a magas kockázat felmérése

A. A kockázat mint bejelentést kiváltó tényező

Az általános adatvédelmi rendelet bevezeti az incidens bejelentésének kötelezettségét, azonban nem írja elő, hogy ennek a kötelezettségnek minden körülmények között eleget kell tenni:

[37] Lásd a 29. cikk szerinti munkacsoport átláthatóságról szóló iránymutatását, amely az aránytalan erőfeszítés kérdéskörével is foglalkozik. A dokumentum a következő internetcímen érhető el: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850

[38] Lásd a 5. cikk (2) bekezdését

- az illetékes felügyeleti hatóságnak való bejelentés kötelező, kivéve, ha az incidens valószínűsíthetően nem jár kockázattal az egyének jogaira és szabadságaira nézve;
- az egyének incidensről való tájékoztatása csak akkor merül fel, ha az incidens valószínűsíthetően magas kockázattal jár az egyének jogaira és szabadságaira nézve.

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

A fentiekben leírtak szerint az incidens bejelentése kötelező, kivéve, ha valószínűsíthetően nem jár kockázattal az egyének jogaira és szabadságaira nézve, az érintettek incidensről való tájékoztatása pedig akkor válik szükségessé, ha valószínűsíthetően *magas* kockázattal jár az egyének jogaira és szabadságaira nézve. Ilyen kockázat akkor merül fel, ha az incidens fizikai, vagyoni vagy nem vagyoni károkat okozhatnak azoknak az egyéneknek, akiknek az adatait az incidens érinti. E károk közé tartozik például a hátrányos megkülönböztetés, a személyazonosság-lopás vagy a személyazonossággal való visszaélés, a pénzügyi veszteség és a jó hírnév sérelme. Amennyiben az incidens a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatokat érint, vagy genetikai adatokra, egészségügyi adatokra, szexuális irányultságára vonatkozó adatokra vagy büntetőjogi felelősség megállapítására vonatkozó határozatokra és a bűncselekményekre, illetve a kapcsolódó biztonsági intézkedésekre vonatkozó adatokra is kiterjed, akkor az ilyen károk valószínűleg bekövetkeznek[39].

B. A kockázat felmérésekor mérlegelendő tényezők

Az általános adatvédelmi rendelet (75) és a (76) preambulumbekezdése utal arra, hogy a kockázat felmérésekor általában az érintettek jogait és szabadságait érintő kockázat valószínűségét és súlyosságát egyaránt figyelembe kell venni. Emellett azt is kimondja, hogy a kockázatot objektív értékelés alapján kell felmérni.

Megjegyzendő, hogy az incidens következtében az egyének jogait és szabadságait fenyegető kockázat felmérése más szempontokra irányul, mint a kockázat adatvédelmi hatásvizsgálat keretében történő felmérése[40]. Az adatvédelmi hatásvizsgálat az adatkezelés terv szerint végrehajtásának kockázataira és az incidens esetén felmerülő kockázatokra egyaránt kiterjed. Az esetleges incidens mérlegelésekor általában véve a bekövetkezésének valószínűségével és az érintettet érő esetleges károkkal foglalkozik, más szóval feltételezett eseményt mér fel. Tényleges incidens esetén már bekövetkezett az esemény, így teljes mértékben az incidens egyénekre gyakorolt hatásából eredő kockázatra kerül a hangsúly.

Példa

Az adatvédelmi hatásvizsgálat szerint egy bizonyos biztonsági szoftvertermék személyes adatok védelmére javasolt használata alkalmas intézkedés arra, hogy megfelelő szintű adatbiztonságot garantáljon ahhoz a kockázathoz mérten, amelyet az adatkezelés egyébként az egyénekre jelentene. Ha azonban utólag fény derül valamilyen sebezhetőségre, azzal megváltozna a szoftver alkalmassága

[39] Lásd a (75) és a (85) preambulumbekezdést.

[40] Lásd a 29. cikk szerinti munkacsoport adatvédelmi hatásvizsgálatokról szóló iránymutatását itt: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137

a védett személyes adatokat fenyegető kockázat elhárítására, így azt a folyamatban lévő adatvédelmi hatásvizsgálat keretében újra fel kell mérni.

A termék sebezhetőségét később valaki kihasználja, és incidens történik. Az adatkezelőnek ekkor meg kell vizsgálnia az incidens konkrét körülményeit, az érintett adatok körét, az egyénekre gyakorolt hatás lehetséges mértékét és a kockázat megvalósulásának valószínűségét.

Ennek megfelelően az adatkezelőnek az egyéneket incidens miatt felmerülő kockázat felmérése során figyelembe kell vennie az incidens konkrét körülményeit, köztük a lehetséges hatás súlyosságát és a bekövetkezésének valószínűségét. A 29. cikk szerinti munkacsoport ezért azt ajánlja, hogy az értékelés során térjenek ki az alábbi kritériumokra[41]:

- Az incidens jellege

A megtörtént incidens jellege befolyásolhatja az egyéneket érintő kockázat mértékét. Például az egyén számára eltérő következményekkel járhat a titoksértés, amelynek keretében jogosulatlan felek egészségügyi információkhoz jutnak, mint az incidens, amelynek keretében az egyén egészségügyi adatai elvesznek vagy hozzáférhetetlenné válnak.

- A személyes adatok jellege, érzékenysége és mennyisége

A kockázat felmérésekor természetesen kulcsfontosságú tényező az incidens által veszélyeztetett személyes adatok jellege és érzékenysége. Rendszerint minél érzékenyebbek az adatok, annál nagyobb a kár bekövetkeztének kockázata az érintett egyének számára, ugyanakkor figyelembe kell venni az érintettről rendelkezésre álló egyéb személyes adatokat is. Például az egyén nevének és címének közlése rendes körülmények között valószínűleg nem okoz jelentős kárt. Ha azonban az örökbefogadó szülő nevét és címét kiadják a vér szerinti szülőnek, ez nagyon súlyos következményekkel járhat az örökbefogadó szülő és a gyermek számára egyaránt.

Az egészségügyi adatokat, személyazonosító okmányokat vagy pénzügyi adatokat, például hitelkártyaadatokat érintő incidensek önmagukban is mind kárt okozhatnak, együttesen azonban személyazonosság-lopáshoz vezethetnek. A személyes adatok rendszerint együttesen érzékenyebbnek tekinthetők, mint külön-külön.

Bizonyos fajta személyes adatok először viszonylag ártalmatlannak tűnhetnek, azonban gondosan mérlegelni kell, mit árulhatnak el az érintett egyénről. A rendszeresen küldeményeket fogadó ügyfelek listája különösebben nem érzékeny, de a nyaralás idejére a küldemények leállítását kérő ügyfelekre vonatkozó hasonló adatok már hasznosak lehetnek a bűnözők számára.

Ehhez hasonlóan kis mennyiségű, fokozottan érzékeny személyes adatnak jelentős hatása lehet az egyénre, és nagy mennyiségű adat információk még szélesebb körét fedheti fel az egyénről. A számos érintettel kapcsolatos, nagy mennyiségű személyes adatot érintő incidens ugyanolyan nagy számú egyénre lehet hatással.

- Az egyének könnyű azonosíthatósága

[41] A 611/2013/EU rendelet 3. cikkének (2) bekezdése iránymutatást nyújt azokról a tényezőkről, amelyeket az elektronikus hírközlési szolgáltatások ágazatában felmerülő incidensek bejelentésével kapcsolatosan mérlegelni kell, és amelyek az általános adatvédelmi rendelet szerinti bejelentéssel összefüggésben is hasznosak lehetnek. Lásd: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:hu:PDF

Fontos, mérlegelendő tényező, hogy a veszélyeztetett személyes adatokhoz hozzáférő fél mennyire könnyen tudja azonosítani az egyes egyéneket, vagy egyének azonosítása céljából más információkkal összeegyeztetni az adatokat. Az azonosításra a körülményektől függően lehetőség nyílhat közvetlenül az incidenssel érintett személyes adatokból, az egyének személyazonosságának felfedésére irányuló különleges kutatás nélkül, de az is előfordulhat, hogy rendkívül nehéz megfeleltetni a személyes adatokat egy bizonyos egyénnek, azonban bizonyos feltételek mellett ekkor is lehetséges. Az azonosítás az incidenssel érintett adatokból közvetlenül és közvetve is megvalósítható, de az incidens sajátos körülményeitől és a kapcsolódó személyes adatok nyilvános hozzáférhetőségétől is függhet. Ez lényegesebb lehet titoksértés és hozzáférhetőségi adatsértés esetén.

A fentiekben leírtak szerint a megfelelő szintű titkosítással védett személyes adatok jogosulatlan személyek számára visszafejtő kulcs nélkül értelmezhetetlenek. Ezenkívül a megfelelően megvalósított álnevesítés (a 4. cikk 5. pontja szerinti fogalommeghatározása: „a személyes adatok olyan módon történő kezelése, amelynek következtében további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik, feltéve hogy az ilyen további információt külön tárolják, és technikai és szervezési intézkedések megtételével biztosított, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet kapcsolni”) is csökkentheti annak a valószínűségét, hogy incidens esetén azonosítani lehessen az egyéneket. Azonban nem tekinthető úgy, hogy az álnevesítési technikák önmagukban értelmezhetetlenné teszik az adatokat.

- Az egyéneket érintő következmények súlyossága

Az incidensben érintett személyes adatok jellegétől függően, például különleges kategóriájú adatok esetében különösen súlyosak lehetnek az egyéneket fenyegető lehetséges károk, különösen akkor, ha az incidens személyazonosság-lopáshoz, személyazonossággal való visszaéléshez, testi sérelemhez, lelki gyötrelemhez, a becsület csorbításához vagy hírnévrontáshoz vezethet. Ha az incidens kiszolgáltatott helyzetben lévő egyének személyes adatait érinti, az ő esetükben nagyobb lehet a károk kockázata.

A lehetséges kockázat mértékére hatással lehet az is, hogy az adatkezelőnek tudomása van-e arról, a személyes adatok ismeretlen vagy rossz szándékú személyekhez kerültek. Titoksértés merülhet fel, amennyiben a személyes adatokat tévedésből közlik a 4. cikk 10. pontjában meghatározott harmadik féllel vagy más címzettel. Ez például akkor fordulhat elő, ha a személyes adatokat véletlenül a szervezet rossz szervezeti egységének vagy széles körben igénybe vett beszállító szervezetnek küldik. Az adatkezelő arra kérheti a címzettet, hogy a kapott adatokat juttassa vissza vagy biztonságosan semmisítse meg. A címzett mindkét esetben „megbízhatónak” tekinthető, amennyiben az adatkezelő folyamatos kapcsolatban áll vele, és ismeri eljárásaikat, történetüket és más fontos részletet. Más szóval az adatkezelő bizonyos mértékig megbízhat a címzettben, így észszerűen várhatja el, hogy a másik fél a tévedésből neki küldött adatokat nem tanulmányozza át, és nem tekint bele, valamint eleget tesz az adatok visszaszolgáltatására vonatkozó utasításoknak. Még ha a címzett be is tekintett az adatokba, az adatkezelő akkor is bízhat abban, hogy további műveleteket nem végez velük, haladéktalanul visszaszolgáltatja őket az adatkezelőnek, és együttműködik a helyreállításukban. Ilyen esetben ez figyelembe vehető az adatkezelő által az incidenst követően elvégzendő kockázatértékelés során: az a tény, hogy a címzett megbízható, nem teszi meg nem történtté az incidenst, csupán mérsékelheti annak súlyosságát. Ugyanakkor ezáltal kiküszöbölhető az egyéneket érintő kockázat valószínűsége, így már nem lesz szükséges a felügyeleti hatóságnak bejelentést tenni vagy az érintett egyéneket értesíteni. Ez szintén esettől függ. Mindazonáltal az adatkezelőnek az incidensek nyilvántartására vonatkozó általános kötelezettsége (lásd a lenti V. szakaszt) részeként ennek ellenére meg kell őriznie az incidensre vonatkozó információkat.

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

- Az egyén sajátosságai

Az incidens érintheti gyermekek vagy más olyan, kiszolgáltatott helyzetben lévő egyének személyes adatait, akik ennek következtében nagyobb veszélybe kerülhetnek. Az egyénnel kapcsolatosan más olyan tényezők is felmerülhetnek, amelyek befolyásolják az incidens rájuk gyakorolt hatását.

- Az adatkezelő sajátosságai

Az adatkezelő és tevékenységei jellege és szerepe befolyásolhatják az incidens következtében az egyéneket érintő kockázat mértékét. Például az egészségügyi szervezetek különleges kategóriájú személyes adatokat dolgoznak fel, következésképpen e személyes adataik megsértése esetén nagyobb fenyegetés éri az egyéneket, mint ha egy újság terjesztési listája kerülne nyilvánosságra.

- Az érintett egyének száma

Az incidens érinthet csak egy, néhány, több ezer vagy akár még több egyént. Általánosságban elmondható, hogy minél nagyobb az érintett egyének száma, annál nagyobb hatást gyakorol az incidens. Az incidens azonban a személyes adatok jellegétől és veszélybe kerülésük körülményeitől függően csupán egyénre is súlyos kihatással lehet. Ismételten az a lényeg, hogy mérlegelni kell az érintettekre gyakorolt hatás valószínűségét és súlyosságát.

- Általános szempontok

Következésképpen a valószínűsíthetően az incidens miatt felmerülő kockázat felmérésekor az adatkezelőnek együttesen kell mérlegelnie az egyének jogaira és szabadságaira esetlegesen gyakorolt hatás súlyosságát és bekövetkezésének valószínűségét. Egyértelmű, hogy amikor az incidens súlyosabb következményekkel jár, a kockázat is magasabb, és ehhez hasonlóan amikor nagyobb ezek bekövetkezésének valószínűsége, akkor a kockázat is fokozódik. Kétség esetén az adatkezelőnek a biztonság kedvéért érdemes inkább bejelentést tenni. A B. melléklet néhány hasznos példával szolgál az egyének számára kockázattal vagy magas kockázattal járó incidensek különböző fajtáira.

Az Európai Uniós Hálózat- és Információbiztonsági Ügynökség (ENISA) ajánlásokat fogalmazott meg az incidensek súlyosságának felmérésére szolgáló módszerről, amelyet az adatkezelők és az adatfeldolgozók hasznosnak találhatnak incidenskezelési tervük kidolgozása során[42].

V. Elszámoltathatóság és nyilvántartás vezetése

A. Az incidensek nyilvántartása

Függetlenül attól, hogy az egyes incidenseket be kell-e jelenteni a felügyeleti hatóságnak, az adatkezelőnek minden incidenst nyilvántartásba kell vennie a 33. cikk (5) bekezdésében foglaltak szerint:

> „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 az e cikk követelményeinek való megfelelést.”

[42] ENISA, Recommendations for a methodology of the assessment of severity of personal data breaches (Ajánlások az adatvédelmi incidensek súlyosságának felmérésére szolgáló módszerről), https://www.enisa.europa.eu/publications/dbn-severity

Ez a rendelkezés összefügg az általános adatvédelmi rendelet elszámoltathatósági elvével, amelyet az 5. cikk (2) bekezdése tartalmaz. A bejelentési kötelezettség alá tartozó incidensek mellett a bejelentési kötelezettség alá nem tartozó incidenseket is az adatkezelő 24. cikk szerinti kötelezettségeivel összefüggő célból kell nyilvántartani, a felügyeleti hatóság pedig betekintést kérhet ebbe a nyilvántartásba. Az adatkezelőket ezért arra biztatjuk, hogy hozzanak létre belső nyilvántartást az incidensekről, amelyek attól függetlenül kerüljenek bele, hogy be kell-e őket jelenteni[43].

Ugyan az adatkezelőnek kell meghatároznia az incidensek nyilvántartásának módszerét és szerkezetét, azonban a rögzítendő adatokat illetően van néhány kulcsfontosságú elem, amelyet minden esetben meg kell adni. Az adatkezelőnek a 33. cikk (5) bekezdésében előírtak szerint nyilván kell tartania az incidensekkel kapcsolatos adatokat, köztük azok okait, a történéseket és az érintett személyes adatok körét. Emellett szerepelnie kell még a nyilvántartásban az incidensek hatásainak és következményeinek, valamint az orvoslásukra tett intézkedéseknek.

Az általános adatvédelmi rendelet nem határozza meg meddig kell megőrizni ezt a nyilvántartást. Amennyiben az ilyen nyilvántartás személyes adatokat tartalmaz, az adatkezelő köteles megállapítani a megfelelő megőrzési időszakot a személyes adatok kezeléséhez kapcsolódó elvek szerint[44] és az adatkezelés jogalapjának megfelelően[45]. A 33. cikk (5) bekezdése szerinti nyilvántartást mindaddig meg kell őriznie, amíg a felügyeleti hatóság felszólíthatja arra, hogy szolgáltasson bizonyítékokat az említett rendelkezés vagy általánosabban az elszámoltathatósági elv betartására. Egyértelmű, hogy amennyiben maga a nyilvántartás nem tartalmaz személyes adatokat, akkor az általános adatvédelmi rendeletben megfogalmazott korlátozott tárolhatósági elv[46] nem vonatkozik rá.

A 29. cikk szerinti munkacsoport azt ajánlja, hogy az adatkezelő az említett adatokon túlmenően az incidensekre válaszként hozott döntései mögötti érvelést is vegye nyilvántartásba. A döntés indoklását különösen akkor kell nyilvántartani, ha az incidenst nem jelentik be. Az indoklásnak tartalmaznia kell azokat az okokat, amiért az adatkezelő úgy véli, hogy az incidens valószínűsíthetően nem jár kockázattal az egyének jogaira és szabadságaira nézve[47]. Ha pedig az adatkezelő szerint teljesül a 34. cikk (3) bekezdésében foglalt valamely feltétel, akkor az adatkezelőnek erre vonatkozóan megfelelő bizonyítékot kell szolgáltatnia.

Amennyiben az adatkezelő bejelenti ugyan az incidenst a felügyeleti hatóságnak, de késik a bejelentéssel, akkor közölnie kell a késedelem okát. Az ezzel kapcsolatosan nyilvántartott információk alapján könnyebben bizonyítható, hogy a bejelentési késedelem indokolt volt, és nem volt túlzott mértékű.

Amikor az adatkezelő incidensről tájékoztatja az érintett egyéneket, átlátható módon kell fogalmaznia, valamint hatékonyan és kellő időben kell tájékoztatást nyújtania. Ennek megfelelően az adatkezelő könnyebben alá tudja támasztani az elszámoltathatóságot és a szabályszerűséget, ha megőrzi e tájékoztatás bizonyítékát.

---

[43] Az adatkezelő dönthet úgy, hogy a 30. cikk értelmében az adatkezelési tevékenységekről vezetett nyilvántartásában rögzíti az incidenseket. Nincs szükség külön nyilvántartásra, amennyiben az incidenssel kapcsolatos információk egyértelműen felismerhetők, és kérésre kigyűjthetők.

[44] Lásd az 5. cikket.

[45] Lásd a 6. és a 9. cikket.

[46] Lásd az 5. cikk (1) bekezdésének e) pontját.

[47] Lásd a (85) preambulumbekezdést.

A 33. és a 34. cikk betartásának megkönnyítése érdekében az adatkezelők és az adatfeldolgozók számára egyaránt előnyös lehet, ha rendelkeznek írásba foglalt bejelentési eljárással, amely meghatározza az incidens észlelése esetén követendő eljárásrendet, így többek között azt, hogyan kell elhárítani és kezelni az incidenseket, elvégezni a helyreállítást, valamint felmérni a kockázatot és bejelenteni az incidenst. Ezzel összefüggésben az általános adatvédelmi rendelet betartásának igazolásához hasznosak lehetnek a bizonyítékok arra vonatkozóan, hogy az alkalmazottak felvilágosítást kaptak ezekről az eljárásokról és mechanizmusokról, valamint tudják, hogyan reagáljanak az incidensekre.

Megjegyzendő, hogy az incidens megfelelő nyilvántartásba vételének elmulasztása esetén előfordulhat, hogy a felügyeleti hatóság gyakorolja az 58. cikk szerinti hatáskörét, illetve a 83. cikk értelmében közigazgatási bírságot szab ki.

B. Az adatvédelmi tisztviselő szerepe

Az adatkezelő vagy az adatfeldolgozó a 37. cikkben előírtak szerint vagy önkéntes alapon, bevált gyakorlatként rendelkezhet adatvédelmi tisztviselővel[48]. Az általános adatvédelmi rendelet 39. cikke több kötelező feladatot is előír az adatvédelmi tisztviselő számára, de azt sem gátolja meg, hogy az adatkezelő adott esetben további feladatokkal bízza meg.

Kifejezetten az incidensbejelentéssel összefüggésben az adatvédelmi tisztviselő kötelező feladatai közé tartozik többek között az adatkezelő vagy az adatfeldolgozó adatvédelmi tanácsokkal és tájékoztatással való ellátása, az általános adatvédelmi rendelet betartásának ellenőrzése, valamint az adatvédelmi hatásvizsgálattal kapcsolatos tanácsadás. Az adatvédelmi tisztviselőnek emellett együtt kell működnie a felügyeleti hatósággal, és kapcsolattartóként kell eljárnia a felügyeleti hatóság és az érintettek felé. Szintén megjegyzendő, hogy a 33. cikk (3) bekezdésének b) pontja előírja az incidens felügyeleti hatóságnak való bejelentése esetére, hogy az adatkezelő közölje az adatvédelmi tisztviselő vagy egyéb kapcsolattartó nevét és elérhetőségeit.

Az incidensek nyilvántartásba vételét illetően az adatkezelő vagy az adatfeldolgozó dönthet úgy, hogy kikéri az adatvédelmi tisztviselő véleményét e nyilvántartás szerkezetéről, összeállításáról és gondozásáról. Az adatvédelmi tisztviselő emellett e nyilvántartás vezetésével is megbízható.

E szempontok alapján nyilvánvaló, hogy az adatvédelmi tisztviselőnek a tanácsadás és a szabályszerűség ellenőrzése révén kulcsszerepet kell játszania az incidensek megelőzésének vagy az incidensekre való felkészülésnek az előmozdításában, valamint az incidensek közben (vagyis a felügyeleti hatóságnak való bejelentéskor) és a felügyeleti hatóság által végzett utólagos vizsgálat során. Erre tekintettel a 29. cikk szerinti munkacsoport azt ajánlja, hogy az adatvédelmi tisztviselőt haladéktalanul tájékoztassák az incidensek bekövetkezése esetén, és vonják be a teljes incidenskezelési és -bejelentési eljárásba.

VI. Más jogi eszközök szerinti bejelentési kötelezettségek

Az adatkezelőknek az incidensek általános adatvédelmi rendelet szerinti bejelentésén és a velük kapcsolatos tájékoztatáson túlmenően, attól elkülönülten ismerniük kell mindazokat a biztonsági incidensek bejelentésére vonatkozó követelményeket, amelyek más kapcsolódó jogszabályok alapján rájuk vonatkozhatnak, és tisztában kell lenniük azzal, ha ezek egyúttal az adatvédelmi incidensek felügyeleti hatóságnak való bejelentésére kötelezik őket. Az ilyen jellegű követelmények tagállamonként eltérőek lehetnek; az alábbi példák azt mutatják be, milyen bejelentési követelmények

[48] Lásd a 29. cikk szerinti munkacsoport adatvédelmi tisztviselőkkel kapcsolatos iránymutatását itt: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

szerepelnek más jogi eszközökben, és ezek hogyan függnek össze az általános adatvédelmi rendelettel:

- 910/2014/EU rendelet a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról (eIDAS-rendelet)[49].

Az eIDAS-rendelet 19. cikkének (2) bekezdése előírja, hogy a bizalmi szolgáltatók értesítik a felügyeleti szervet a biztonság megsértéséről vagy az adatok sértetlenségének megszűnéséről, amennyiben az jelentős hatást gyakorol a bizalmi szolgáltatásra vagy az annak keretében tárolt személyes adatokra. Adott esetben – vagyis akkor, ha a biztonság megsértése vagy az adatok sértetlenségének megszűnése az általános adatvédelmi rendelet értelmében egyúttal adatvédelmi incidensnek minősül – a bizalmi szolgáltatónak bejelentést kell tennie a felügyeleti hatóságnak is.

- (EU) 2016/1148 irányelv a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről (kiberbiztonsági irányelv)[50].

A kiberbiztonsági irányelv 14. és 16. cikke előírja, az alapvető szolgáltatásokat nyújtó szereplők és a digitális szolgáltatók bejelentsék a biztonsági incidenseket az illetékes hatóságnak. A kiberbiztonsági irányelv (63) preambulumbekezdése[51] elismeri, hogy a biztonsági incidensek során gyakran személyes adatok kerülnek veszélybe. A kiberbiztonsági irányelv ugyan előírja, hogy az illetékes hatóságok és a felügyeleti hatóságok működjenek együtt, és ennek keretében folytassanak információcserét, változatlanul érvényes, hogy amennyiben az ilyen incidensek az általános adatvédelmi rendelet szerinti adatvédelmi incidensnek minősülnek vagy azzá válnak, akkor az említett szereplőknek, illetve szolgáltatóknak a kiberbiztonsági irányelv incidensbejelentési követelményeitől elkülönülten a felügyeleti hatóságnak is bejelentést kell tenniük.

Példa

Előfordulhat, hogy a kiberbiztonsági irányelv szerinti incidenst bejelentő felhőszolgáltatónak az adatkezelőt is értesítenie kell, ha ez az incidens adatvédelmi incidenssel jár együtt. Ehhez hasonlóan az is előfordulhat, hogy az eIDAS-rendelet szerint bejelentést tevő bizalmi szolgáltatónak incidens esetén az illetékes adatvédelmi hatóságnak is bejelentést kell tennie.

- a 2009/136/EK irányelv (a polgárok jogairól szóló irányelv) és a 611/2013/EU rendelet (az incidensek bejelentéséről szóló rendelet).

A 2002/58/EK irányelv értelmében nyilvánosan elérhető elektronikus hírközlési szolgáltatást nyújtó szolgáltatóknak[52] be kell jelenteniük az incidenseket az illetékes nemzeti hatóságoknak.

---

[49] Lásd: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.HUN

[50] Lásd: http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.HUN

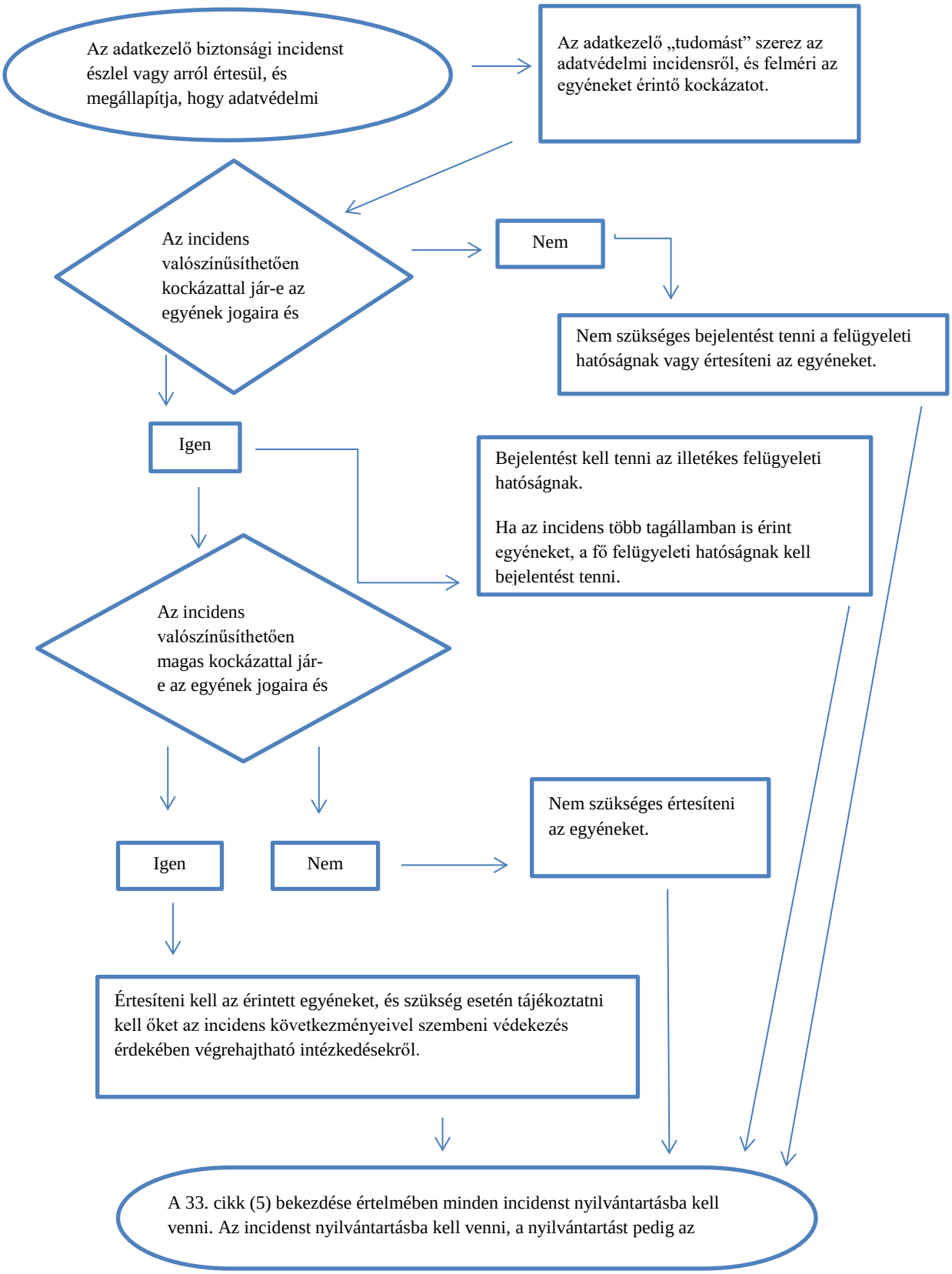
51 A (63) preambulumbekezdés: *„A biztonsági események kapcsán sok esetben személyes adatok kerülnek veszélybe. Ebben az összefüggésben az illetékes hatóságoknak és az adatvédelmi hatóságoknak együtt kell működniük és információt kell cserélniük egymással minden vonatkozó kérdésről, hogy fel lehessen venni a küzdelmet a személyes adatok biztonsági eseményekből eredő bármely megsértése ellen.”*

[52] 2017. január 10-én az Európai Bizottság a magánélet tiszteletben tartásáról és az elektronikus hírközlésről szóló rendeletre tett javaslatot, amely majd a 2009/136/EK irányelv helyébe lép, és megszünteti a bejelentési követelményeket. Amíg azonban az Európai Parlament jóvá nem hagyja ezt a javaslatot, addig a jelenlegi bejelentési követelmény hatályban marad. Lásd: https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications

Az adatkezelőknek a más vonatkozó szabályozás alapján fennálló további jogi, egészségügyi vagy szakmai bejelentési kötelezettségeket is ismerniük kell.

VII. **Melléklet**

A. Folyamatábra a bejelentési kötelezettségekről



B. Példák adatvédelmi incidensekre és az értesítendő felekre

Az alábbi táblázat a teljesség igénye nélkül mutat be példákat, amelyek alapján az adatkezelők könnyebben megállapíthatják, hogy az adatvédelmi incidens különféle eseteiben kell-e bejelentést tenniük. Az alábbi példák az egyének jogait és szabadságait érintő kockázat és magas kockázat megkülönböztetésében is segítséget jelenthetnek.

Példa	**Bejelentendő a felügyeleti hatóságnak?**	**Értesítendő az érintett?**	**Megjegyzések/ajánlások**
i. Az adatkezelő USB-kulcson tárolta a titkosított személyes adatok archívumának biztonsági másolatát. A kulcsot betörés során ellopják.	Nem.	Nem.	Amíg az adatokat a legkorszerűbb algoritmussal titkosítják, vannak biztonsági másolatok az adatokról, az egyedi kulcs nem kerül veszélybe, és az adatok időben helyreállíthatók, addig ezt az incidenst nem kell bejelenteni. Ha azonban a későbbiekben veszélybe kerülnek az adatok, akkor bejelentést kell tenni.
ii. Az adatkezelő internetes szolgáltatást üzemeltet. A szolgáltatás ellen intézett kibertámadás következtében egyének személyes adatai szivárognak ki. Az adatkezelőnek egyetlen tagállamban vannak ügyfelei.	Igen, bejelentést kell tenni a felügyelő hatóságnak, ha valószínűsíthetően az egyéneket érintő következmények merülnek fel.	Igen, az érintett személyes adatok jellegétől függően és a valószínűsíthetően az egyéneket érintő fokozottan súlyos következmények esetén értesíteni kell az egyéneket.	
iii. Az adatkezelő telefonos ügyfélszolgálatán rövid, néhány perces áramkimaradás történik, amelynek következtében az ügyfelek nem tudják felhívni az adatkezelőt és nem tudnak hozzáférni a nyilvántartott adataikhoz.	Nem.	Nem.	Ez nem bejelentendő incidens, mindazonáltal a 33. cikk (5) bekezdése értelmében nyilvántartásba kell venni. Az adatkezelőnek megfelelő nyilvántartást kell vezetnie.
iv. Az adatkezelőt	Igen, bejelentést kell	Igen, az érintett	Ha rendelkezésre

zsarolóvírust támadás éri, amely az összes adatát titkosítja. Nem állnak rendelkezésre biztonsági másolatok, és az adatok nem állíthatók helyre. A vizsgálat során egyértelművé válik, hogy a zsarolóvírus kizárólagos funkciója az adatok titkosítása volt, és nincs más rosszindulatú program a rendszerben.	tenni a felügyelő hatóságnak, ha valószínűsíthetően az egyéneket érintő következmények merülnek fel, mivel ez az eset a hozzáférhetőség elveszésének minősül.	személyes adatok jellegétől és az adatok hozzáférhetőségének elvesztése által esetlegesen gyakorolt hatástól, valamint más valószínűsíthető következményektől függően értesíteni kell az egyéneket.	állnának biztonsági másolat, és az adatok időben helyreállíthatók lennének, akkor ezt az esetet nem lenne szükséges bejelenteni a felügyeleti hatóságnak, és az egyéneket sem lenne szükséges értesíteni róla, mivel nem veszett volna el véglegesen a hozzáférhetőség vagy a titkosság. Ha azonban a felügyeleti hatóság más módon tudomást szerez az incidensről, akkor vizsgálat lefolytatását ítélheti szükségesnek a 32. cikkben foglalt szélesebb körű biztonsági követelmények teljesítésének értékelése céljából.
v. Egy egyén felhívja az egyik bank telefonos ügyfélszolgálatát, hogy adatvédelmi incidenst jelentsen be. Az egyén valaki más havi számlakivonatát kapta meg. Az adatkezelő rövid (24 órán belül lezáruló) vizsgálatot végez és észszerű bizonyossággal megállapítja, hogy adatvédelmi incidens történt, és azt, hogy olyan rendszerszintű hiba fordult-e elő, amely más egyéneket is érint vagy érinthet.	Igen.	Csak az érintett egyéneket kell értesíteni, ha magas a kockázat, és egyértelmű, hogy mások nem érintettek.	Ha további kivizsgálás után megállapítást nyer, hogy több egyén érintett, naprakész tájékoztatást kell adni a felügyeleti hatóságnak, az adatkezelőnek pedig intézkednie kell a többi egyén értesítéséről, amennyiben magas kockázat fenyegeti őket.
vi. Az adatkezelő online piacteret üzemeltet, és több országban is vannak vásárlói. A piactér	Igen, határokon átnyúló adatkezelés esetén a fő felügyeleti hatóságnak kell	Igen, mivel magas kockázathoz vezethet.	Az adatkezelőnek fel kell lépnie, például kötelezővé kell tennie új jelszó beállítását az érintett fiókokhoz,

kibertámadást szenved, és a támadó felhasználóneveket, jelszavakat és vásárlási előzményeket tesz közzé az interneten.	bejelentést tenni.		emellett további kockázatcsökkentő intézkedéseket kell tennie. Az adatkezelőnek azt is meg kell vizsgálnia, hogy vannak-e egyéb bejelentési kötelezettségei, például digitális szolgáltatóként a kiberbiztonsági irányelv alapján.
vii. Egy adatfeldolgozóként eljáró webtárhely-szolgáltató vállalkozás hibát fedez fel a felhasználói hitelesítést vezérlő programkódban. A hiba következtében akármely felhasználó hozzáférhet bármely más felhasználó fiókadataihoz.	A webtárhely-szolgáltató vállalkozásnak adatfeldolgozóként indokolatlan késedelem nélkül értesítenie kell az érintett ügyfeleit. Feltéve, hogy a webtárhely-szolgáltató vállalkozás végzett saját vizsgálatot, az érintett adatkezelő észszerűen bizonyosak lehetnek abban, hogy mindegyikük adatvédelmi incidenst szenvedett el, ezért valószínűsíthető, hogy „tudomásukra jutott” az incidens, miután értesítette őket a tárhelyszolgáltató vállalkozás (az adatfeldolgozó). Az adatkezelőknek ekkor bejelentést kell tenniük a felügyelő hatóságnak.	Ha valószínűsíthetően nem merül fel jelentős kockázat az egyének számára, akkor őket nem szükséges értesíteni.	Az A webtárhely-szolgáltató vállalkozásnak (az adatfeldolgozónak) meg kell vizsgálnia, hogy vannak-e egyéb bejelentési kötelezettségei, például digitális szolgáltatóként a kiberbiztonsági irányelv alapján. Ha nincs bizonyíték arra, hogy ez a sebezhetőséget bármely adatkezelőnél kihasználták volna, akkor az incidenst nem szükséges bejelenteni, ugyanakkor valószínűleg nyilvántartásba kell venni, vagy a 32. cikk be nem tartásának kell tekintheti.
viii. Az egyik kórházban kibertámadás miatt harminc órára hozzáférhetetlenné vált az egészségügyi nyilvántartás.	Igen, a kórház köteles bejelentést tenni, mivel jelentős kockázat merülhet fel a betegek jóllétére és magánéletére nézve.	Igen, értesíteni kell az érintett egyéneket.	

ix. Jelentős számú tanuló személyes adatait véletlenül téves, több mint ezer címzettet tartalmazó levelezőlistára küldik el.	Igen, bejelentést kell tenni a felügyeleti hatóságnak.	Igen, az érintett személyes adatok körétől és jellegétől, valamint a lehetséges következmények súlyosságától függően értesíteni kell az egyéneket.	
x. Közvetlen üzletszerzési célú e-mailt küldenek a „Címzett” vagy a „Másolatot kap” mezőben megadott címzetteknek, ezzel lehetővé téve, hogy mindegyik címzett lássa a többi címzett e-mail címét.	Igen, a felügyeleti hatóságnak való bejelentés kötelező lehet, ha nagyszámú egyén érintett, különleges adatok kerülnek nyilvánosságra (például pszichoterapeuta levelezőlistája), vagy más tényezők miatt merül fel magas kockázat (például a levél tartalmazza a kezdeti jelszavakat).	Igen, az érintett személyes adatok körétől és jellegétől, valamint a lehetséges következmények súlyosságától függően értesíteni kell az egyéneket.	Előfordulhat, hogy nincs szükség bejelentésre, ha csak kevés e-mail cím kerül nyilvánosságra, különleges adatok pedig nem.