JOGI FÓRUM PUBLIKÁCIÓ

www.jogiforum.hu

**Dr. Domokos N. Márton:**

# *„Tényleg azt hiszi, hogy minden információ nélkül részt veszek ebben?"*

**avagy**

## Adatbiztonsági értesítési szabályok, kérdések és gyakorlati tanácsok

## I. BEVEZETÉS

*„Csak töltse ki a formanyomtatványokat. Jelentkezési lap, pszichológiai teszt. M.M.P.I és T.A.T tesztek. A pénzügyi kérdésekre ne válaszoljon, ha nem akar. Mindössze a képességeit akarjuk felmérni, a korlátait, hogy mi érdekli, és mi nem…"*

*„Tényleg azt hiszi, hogy minden információ nélkül részt veszek ebben?"*

*„Először is, ismerje be, hogy érdekesnek hangzik. Másodszor, nem kell ma döntenie. Csak csinálja meg a rutinteszteket, töltse ki a nyomtatványokat. Bármikor kiszállhat, minden kötelezettség nélkül."*

Így kezdődött – Nicholas van Orton (Michael Douglas alakításában a „Játszma" című filmben) csak pár személyiségtesztet töltött ki, de az így átadott információkat felhasználva egy lenyomozhatatlan szervezet azonnal átvette az irányítást magánszférája (és a bankszámlája) felett. A személyes adatait elvesztett Nicholas végül egy koporsóban tért magához, élve eltemetve egy mexikói faluban.

Szerencsére a személyes adatokkal való ennyire durva visszaélés egyelőre csak David Fincher thrillerjeiben történhet meg – talán köszönhetően többiek között annak is, hogy ma már az Amerikai Egyesült Államok (USA) legtöbb tagállamában részletes, úgynevezett „adatbiztonsági értesítési kötelezettségekre vonatkozó jogszabályt" (*security breach notification laws*) fogadtak el. 2011. május 25-ig az Európai Unió (EU) tagállamainak is hasonló – igaz, az amerikainál jóval kevésbé kidolgozott – szabályokat kellett hatályba léptetniük, az Európai Parlament és a Tanács 2009/136/EK – 2009. november 25. – irányelvével módosított (Módosító Irányelv) „e-Privacy Irányelv"[1] értelmében.

[1] Az Európai Parlament és a Tanács 2002/58/EK (2002. július 12.) az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről szóló irányelve – módosította az Európai Parlament és a Tanács 2009/136/EK - 2009. november 25. irányelve.

A jelen írás egy, a bostoni Suffolk University Law School részére végzett kutatási projekt kivonata. Célja, hogy általános képet adjon az USA[2] és az EU adatbiztonsági értesítési kötelezettségekre vonatkozó jogszabályairól, rövid kitekintéssel gyakorlati alkalmazásukra. Ezt követően az írás kitér az adatbiztonsági értesítésekkel kapcsolatos gyakorlati tanácsokra (adatkezelők részére) és a várható szabályozási fejleményekre. Terjedelmi okokból nincs arra lehetőség, hogy részletesen bemutatásra kerüljön a vonatkozó teljes joganyag és esetjog, ezért - a kutatás pontosságának és teljességének biztosítása érdekében tett erőfeszítések ellenére - természetesen az írás nem helyettesíti a megfelelő jogi tanácsot.

## 1. Háttér

Köztudott, hogy mind az állami, mind a magánszektor egyre nagyobb mennyiségű személyes adatot kezel. A gyakorlatban szükségszerűen adatkezeléssel járnak az olyan mindennapos tevékenységek, mint például a hitelkártya-információk továbbítása, nyilvános adatbázisokból való adatkérés, vásárlási szokásokról szóló kérdőívek kitöltése, jótállási feltételek online regisztrációja, vagy akár bármilyen internetes honlap használata. Ezek a tevékenységek mind-mind ideális célpontok az elvesztett vagy ellopott személyes adatokat jogosulatlan célokra (pl. fizetési kötelezettségek vállalására) használó adatvadászok számára.

A személyiséglopás (*identity theft*) jellegű bűncselekmények vagy az adatokkal való egyéb visszaélések száma világszerte nő, és az emberek magánszférája, személyes adataik biztonsága egyre több veszélynek van kitéve. Ha a személyes adatok veszélybe kerülését vagy sérelmét (adatbiztonsági esemény) az adatkezelők, az adatgazdák és az illetékes hatóságok nem kezelik megfelelő időben és módon, megnő a kockázata annak, hogy az adatkezelő birtokából kikerült személyes adatok ténylegesen jogosulatlanul kerülnek felhasználásra és ezzel végső soron az adatkezelő és az adatgazda érdekkörében is jelentős kár merülhet fel.

## 2. Az adatbiztonsági események okai és következményei

Az adatbiztonsági események okai legtöbbször az adatkezeléssel érintett IT hálózatba való külső behatolás, vagy az adatkezelő szervezetén belüli bűncselekmény, gondatlanság (pl. fájlok nem

[2] A vonatkozó jogszabályhelyekre vezető link elérhető az alábbi honlapon: http://www.ncsl.org/programs/lis/cip/priv/breach.htm és egy rövid összehasonlítás itt: http://www.scottandscottllp.com/resources/state_data_breach_notification_law.pdf

megfelelő kezelése vagy továbbítása, adatok véletlen internetes közzététele), dokumentumok vagy az azokat tároló hardver ellopása vagy elvesztése. Az adatkezelők számára jelentős költségeket okozhat az adatbiztonsági eseményekhez kapcsolódó általános válságmenedzsment - belső vizsgálatok, ügyfélértesítések, a jogszabályi megfelelőség (*compliance*) helyreállítása, valamint a megfelelő technikai-biztonsági intézkedések megtételének elmulasztása miatt a károsultak által indított perekben való védekezés.

Egy legutóbbi tanulmány[3] szerint 2009-ben egy-egy adatbiztonsági eseménnyel kapcsolatban az átlagköltség 6,75 millió USD volt, amely durva becsléssel átlagosan ügyfelenként körülbelül 204 USD költséget jelentett. Egy másik tanulmány a vizsgált hat éves időszakban (2005-2010) nyilvánosságra hozott 3765 adatbiztonsági esemény összköltségét 156,7 milliárd USD összegre becsülte.[4]

Az érintett vállalkozásoknak a negatív publicitás, az ügyfelek bizalmának elvesztése és az átlátható működés hiánya is versenyhátrányt okozhat. Adatbiztonsági eseményekre ugyanakkor a legváratlanabb módokon is sor kerülhet, például a nem megfelelően lesejtezett fénymásolók adattároló alkatrészeiből hozzáférhető adatok kinyerésével – egy massachusettsi törvénytervezet szerint ennek elkerülése érdekében külön figyelemfelhívó jelzést kellene rakni az ilyen gépekre.[5]

## 3. A megfelelő háttértudás és felkészültség hiánya

Egy nemrég publikált tanulmány szerint[6] a pénzügyi vezetők 95%-a sajnos nem ismeri az IT rendszereket fenyegető veszélyeket, és a cégeknek csak a fele rendelkezik IT biztonsági tervekkel. Az adatbiztonsági események növekvő száma miatt fontos, hogy az adatkezelők ne csökkentsék az IT biztonsági rendszerük bevezetésére és továbbfejlesztésére költött összegeket, ugyanis egy adatbiztonsági esemény által okozott kár jelentősen meghaladhatja a látszólag megspórolt fejlesztési költségeket.[7]

## 4. Gyakorlati példák adatbiztonsági eseményekre

Lássunk néhány példát az USA-ból.

---

[3] **The Cost of a Data Security Breach** http://blog.alertsec.com/2010/02/the-cost-of-a-data-security-breach/

[4] **Data breaches cost organizations a staggering $156.7 billion over six years** http://www.infosecurity-us.com/view/20563/data-breaches-cost-organizations-a-staggering-1567-billion-over-six-years/

[5] **Data Security Evil Lurking Inside Copiers - New Law to the Rescue?** http://blog.hrwlawyers.com/blog/bid/53342/data-security-evil-lurking-inside-copiers-new-law-to-the-rescue

[6] **The Financial Management of Cyber Risk** http://webstore.ansi.org/cybersecurity.aspx

[7] Lásd még: **Pénzügyi karanténban az informatikai biztonság** http://www.bitport.hu/biztonsag/penzugyi-karantenben-az-informatikai-biztonsag

Az **egészségügyi szektor** különösen veszélyeztetett – ráadásul, egy nemrég közzétett tanulmány szerint, az adatbiztonsági események legnagyobb részét az adatkezelők saját munkavállalói okozzák azzal, hogy kollégáik, rokonaik vagy barátaik egészségügyi adataiba néznek bele jogosulatlanul![8]

Jellemző esetek még:

- A Providence Home Services egyik munkatársa 2005. december 31-én archív anyagokat hagyott éjszakára a háza előtt parkoló gépkocsijában. A 365.000 páciens személyes adatát (pl. társadalombiztosítási szám, születési időpont, lakcím, egészségügyi adatok) tartalmazó anyagokat ellopták.[9]
- 2006-ban a szövetségi Veterans Administration által kezelt 26,5 millió veterán és házastársaik személyes adatai kerültek illetéktelen kezekbe, amikor az adatkezelő egyik munkatársának laptopját ellopták otthonából.[10]
- 2009 novemberében egy másik egészségügyi szervezet, a Blue Cross Blue Shield bizalmas információi (pl. 800.000 személy adó- és társadalombiztosítási azonosítószáma) egy laptop ellopása következtében szintén illetéktelen kezekbe kerültek.[11]
- A Health Net nevű egészségügyi szolgáltató egyik munkatársa 2009 márciusában elvesztett egy pendrive-ot, amely nem titkosítva 1,5 millió páciens és 5000 orvos adatát (társadalombiztosítási azonosítók, bankszámlaszámok, egészségügyi adatok) tartalmazta. A több tagállamra is kiterjedő adatbiztonsági eseményre hat hónappal később derült fény – a szolgáltató állítása szerint az adatokhoz ugyanakkor csak speciális, a szolgáltató számára elérhető szoftverrel lehetett hozzáférni. Az ügyben eljáró ügyész sajtónyilatkozatában megjegyezte: *„a cégek még mindig nem értik – a személyes adatra úgy kell vigyázni, mint a készpénzre!”*[12]
- A California Department of Health 2010 februárjában küldött adatbiztonsági értesítést arról, hogy tévedésből körülbelül 50.000 személy társadalombiztosítási azonosítója

[8] **Over 70% of Healthcare Providers Suffered Privacy Breaches** http://blog.veriphyr.com/2011/08/over-70-of-healthcare-providers.html

[9] **Four lose jobs after data breach at Oregon health care facility** http://www.computerworld.com/s/article/109067/Four_lose_jobs_after_data_breach_at_Oregon_health_care_facility

[10] **Veterans Affairs warns of massive privacy breach** http://www.securityfocus.com/news/11393

[11] **Blue Cross Blue Shield Data Breach Investigated** http://www.informationweek.com/news/healthcare/security-privacy/showArticle.jhtml?articleID=221601331

[12] **Health Insurer Loses 1.5 Million Patient Records** http://www.wired.com/threatlevel/2009/11/healthnet/

került rá véletlenül a számukra küldött levelek címzésére.[13]

- Még súlyosabb eset volt szintén 2011 júniusában, amikor egy suffolki pszichiáter az általa kezelt beteg kezelésével kapcsolatos információkat átadta a beteg leendő munkáltatója egyik megbízottjának. A cselekmény Virginia jogszabályai alapján akár öt év szabadságvesztéssel is büntethető.[14]
- 2011 júliusában az állami társadalombiztosítási szerv egyik munkavállalója ellen emeltek vádat, mert állítólag jogosulatlanul gyűjtött és továbbított munkájának ellátásához nem szükséges adatokat a társadalombiztosítási adatbázisból.[15]

A **pénzügyi szektor** szintén rendkívül veszélyeztetett.[16]

- Albert Gonzalez (egykori titkosszolgálati informátor) két társával betört a hitelkártya-üzletágban működő New Jersey-beli Heartland Payment Systems, valamint a Hannaford Brothers, a 7-Eleven és két másik kereskedő számítógépes rendszerébe és állítólag több mint 130 millió hitel- és betéti kártya adatot loptak el. Az érintett cégeket ért kár eddig 12.600.000 USD, ideértve a jogi költségeket és a fizetési eszközökkel kapcsolatos biztonsági szabályoknak való nem-megfelelés (pl. a wireless hálózat sebezhetősége) miatt kiszabott pénzbüntetéseket.[17] Állítólag ugyanez a személy volt értintett az egyik legsúlyosabb adatbiztonsági eseményben (az úgynevezett „TJX" ügyben), ahol mintegy 95.000.000 hitelkártyaadat került veszélybe.[18]
- A Downeast Energy & Building Supply 2009 szeptemberében körülbelül 850 ügyfelét tájékoztatta arról, hogy a társaság online bankszámláját hackerek törték fel, elloptak 200.000 USD-t és az ügyfelek személyes adataihoz is hozzáfértek.[19]
- A Chase Bank szintén 2009 szeptemberében ismeretlen számú ügyfélnek küldött adatbiztonsági értesítést azt követően, hogy egy, az ügyfelek személyes adatait

[13] **Security Breach Exposes Healthcare Recipients' Data** http://www.informationweek.com/news/healthcare/security-privacy/showArticle.jhtml?articleID=222700692

[14] **Doctor indicted for disclosing health information** http://www.wavy.com/dpp/news/crime/doctor-indicted-for-disclosing-health-information

[15] **Social Security Employee Steals Personal Information for Identity Theft** http://www.2removespyware.com/2011/07/31/social-security-employee-steals-personal-information-for-identity-theft/

[16] Egy interaktív időrenddel párosított statisztika szerint 2009. december 31-ig az USA-ban található pénzügyi intézmények közül 62-nél merült fel adatbiztonsági esemény. **2009 Data Breaches: An Interactive Timeline** http://www.bankinfosecurity.com/articles.php?art_id=1766

[17] **TJX Hacker Charged With Heartland, Hannaford Breaches** http://www.wired.com/threatlevel/2009/08/tjx-hacker-charged-with-heartland/

[18] **TJX (T.J. Maxx) reaches settlement with states on Data Loss** http://simonhunt.wordpress.com/2009/06/24/tjx-t-j-maxx-reaches-settlement-with-states-on-data-loss/

[19] **Downeast Energy Suffers Security Breach** http://www.databreaches.net/?p=7136

tartalmazó adattároló eszköz eltűnt egy szerződéses partner archívumából.[20]

Az **oktatási rendszerben** kezelt személyes adatok is veszélyben lehetnek.

- 2008 és 2009 között, hat hónapon keresztül, hackerek jogosulatlanul hozzáfértek a University of California, Berkeley szervereihez, és 160.000 diák, öregdiák és szülő személyes adatát lopták el.[21]
- 2009 júniusában a Cornell egyetem 45.000 munkatársának és diákjának egy laptop-on nem titkosított formában tárolt személyes adatai kerültek veszélybe, miután a nem megfelelő helyen tárolt laptopot ellopták.[22]
- A Yale egyetem 2011 szeptemberének elején 43.000 személyt értesített arról, hogy nevük és társadalombiztosítási azonosítójuk – az adattároló FTP szerveren keresztül – 10 hónapig nyilvánosan elérhető volt Google-keresésen keresztül.[23]

Adatbiztonsági események természetesen **más iparágakban** is előfordulnak.

- Az úgynevezett „Jetblue" ügyben az illetékes hatóság (*Transportation and Security Administration*) arra kérte a JetBlue-t, hogy egy légitársasági adatokkal kapcsolatos, adatfeltáró és elemző program próbaüzemének futtatása érdekében utasainak helyfoglalás-visszaigazolási számát továbbítsa egy másik állami szerv (*Department of Defense*) szerződéses partnere részére. A JetBlue ezt követően saját adatvédelmi szabályzatát megszegve – amelyben vállalta, hogy a harmadik feleknek nem továbbít személyes adatokat - nagy mennyiségű ügyféladatot továbbított a szerződő partnernek. Megtévesztésre, szerződésszegésre és a magánélet megsértésére hivatkozással a társaság ellen ügyfelei pert indítottak, és az Elctronic Privacy Information Center nevű adatvédelmi jogi csoport is panasszal élt a Szövetségi Kereskedelmi Bizottságnál (*Federal Trade Commission*), mivel a légitársaság megszegte az ügyfelek adatvédelme

[20] **Chase Bank Notifies Customers of Breach** http://stopidtheftcrime.blogspot.com/2009/09/chase-bank-notifies-customers-of-breach.html

[21] **UC Berkeley Health Service Data Stolen By Overseas Criminals** http://www.informationweek.com/news/security/attacks/showArticle.jhtml?articleID=217400055

[22] **Security Breach Leaves 45,000 at Risk of Identity Theft** http://cornellsun.com/section/news/content/2009/06/24/security-breach-leaves-45000-risk-identity-theft

[23] **Yale warns 43,000 about 10-month-long data breach** http://www.computerworld.com/s/article/9219369/Yale_warns_43_000_about_10_month_long_data_breach

kapcsán tett vállalásait.[24]

- Az adatbiztonsági események az egyre népszerűbb felhőalapú-szolgáltatásokat (*cloud computing services*) is érinthetik: a vonatkozó kaliforniai adatvédelmi jogszabályok alapján indult csoportos kereset a Dropbox., Inc. nevű felhőszolgáltató ellen, mert elmulasztotta az általa tárolt személyes adatokkal kapcsolatban a megfelelő adatbiztonsági intézkedések megtételét, majd a körülbelül 25 millió (!) előfizető értesítését az adatbiztonsági eseményről. Az esemény során az előfizetők beléphettek más előfizetők fiókjába, és hozzáférhettek az ott tárolt adatokhoz.[25]
- Az Epsilon nevű – például a JP Morgan Chase vagy a Brookstone e-mail kommunikációjáért felelős - szolgáltató adatbázisába 2011. március 30-án törtek be. Komolyabb jogsérelemről egyelőre nincs információ, de az eseményt már csak az érintett adatok száma miatt is érdemes megemlíteni: a cégen 40 milliárd e-mail fut keresztül évente.[26] Az Epsilon anyavállalatának becsült kára az adatbiztonsági esemény következtében 100 millió USD (árbevételének 4%-a)!
- 2011 áprilisában a Sony Playstation Networks 77 millió online felhasználójának adataihoz fértek hozzá hackerek – az esettel kapcsolatban felmerült az adatkezelő által újonnan bevezetett szoftverek biztonsági szintjének, és a felhasználók számára küldött értesítés gyorsaságának nem-megfelelősége is.[27]
- 2011 júniusában hackerek fértek hozzá a Bioware számítógépes játék-gyártó adatbázisában tárolt 18.000 ügyfél adatához, például felhasználónevekhez, titkosított jelszavakhoz, email-címekhez, levelezési címekhez – egy, az üggyel foglalkozó írás ugyanakkor leginkább amiatt aggódott, hogy emiatt késni fog a Mass Effect 3. című játék megjelenése.[28]
- Az adatbiztonsági események következménye akár fizikai bántalmazás is lehet. A New Hampshire-i Legfelsőbb Bíróság például 2003-ban a *Remsburg v. Docusearch, Inc.* ügyben megállapította, hogy a személyes adatok adásvételével foglalkozó személy

---

24 **Airline passengers file lawsuit against JetBlue Airways for invasion of privacy** http://www.allbusiness.com/operations/shipping-air-freight/645014-1.html

25 **Class Action Suit Filed Against Cloud Service over Data Breach** http://www.xydo.com/toolbar/24849928-class_action_suit_filed_against_cloud_service_over_data_breach

26 **Epsilon Notifies Clients of Unauthorized Entry into Email System** http://www.epsilon.com/News%20%26%20Events/Press_Releases_2011/Epsilon_Notifies_Clients_of_Unauthorized_Entry_into_Email_System/p1057-l3

27 **Sony PlayStation suffers massive data breach** - http://www.reuters.com/article/2011/04/26/us-sony-stoldendata-idUSTRE73P6WB20110426; **Sony sued for PlayStation Network data breach** http://news.cnet.com/8301-31021_3-20057921-260.html

28 **Heads Up, Geeks and Gamers: Bioware is the Latest Data Breach Victim** http://www.abine.com/wordpress/2011/heads-up-geeks-and-gamers-bioware-is-the-latest-data-breach-victim/

felelős lehet a személyes adatok megfelelő körültekintés nélkül történő eladásából származó károkért. Az ügyben a Docusearch Inc. nevű cég eladta Amy Boyer magánszemély munkahelyi címét és egyéb személyes adatait. A vevő – Amy Boyer középiskolai osztálytársa, aki weboldalán naplót vezetett a lánnyal kapcsolatos vonzalmáról, és arról, hogy a lányt bántalmazni fogja – a megszerzett adatok alapján kinyomozta a munkából hazainduló lány tartózkodási helyét és megölte.[29]

## 5. Európai példák

Lássunk pár európai példát is.

- 2007-ben két, gyermekekkel kapcsolatos juttatások adatbázisát (25 millió magánszemély és 7,25 millió család személyes adatát) tartalmazó adathordozó tűnt el az angol HM Revenue & Customs belső kézbesítési rendszerében. Szerencsére úgy tűnik, hogy az érintett különleges személyes adatok nem kerültek jogosulatlan személyekhez, mindesetre az érintett személyeket figyelmeztették bankszámlájuk fokozottabb figyelésére. Ezen felül a HM Revenue & Customs-öt bírálták a megfelelő adatvédelmi eljárás hiányáért, különösen, mert a különleges adatokat nem kellett volna cd-ken köröztetni.[30]
- 2008 elején az angol Marks and Spencer 26.000 munkavállalójának személyes adatai kerültek veszélybe egy laptop ellopása következtében. Az Egyesült Királyság adatvédelmi hatósága – Information Commissioner's Offce (ICO) – utasította a Marks and Spencert, hogy biztosítsa az általa kezelt személyes adatok titkosítását.[31]
- Az Egyesült Királyságban még az adatbiztonsági értesítések kötelező törvényi szabályozásának bevezetését megelőzően az HSBC-t a pénzügyi felügyelet – Financial Services Authority (FSA) - 5.000.000 GBP-re bírságolta a személyes adatok védelmének két alkalommal való elmulasztása miatt. [32] 2007 áprilisában az HSBC Actuaries 1.917 nyugdíjpénztári tag nem titkosított személyes adatait (cím, születési dátum és társadalombiztosítási szám) tartalmazó adathordozót vesztett el. Az FSA a HSBC

[29] Más ügyekkel együtt elemzi: **Anita Ramasastry**: **Data Insecurity: What Remedy Should Consumers Have When Companies Do Not Keep Their Data Safe?** http://writ.news.findlaw.com/ramasastry/20060306.html

[30] **UK's families put on fraud alert** http://news.bbc.co.uk/2/hi/7103566.stm

[31] **M&S 'data protection breach** http://www.telegraph.co.uk/news/uknews/1576604/MandS-data-protection-breach.html

[32]

Insurance Brokers-t is megbüntette, mert a vonatkozó adatvédelmi jogszabályt megszegve elmulasztott biztonsági intézkedéseket tenni a kérdéses adatok védelme érdekében, és nem tartotta be az FSA „Üzleti iránymutatásai" közül a 3. számú adatbiztonsági iránymutatást sem, miszerint az adatkezelőnek megfelelő kockázatkezelési rendszer bevezetésével meg kell tennie a szükséges intézkedéseket a működésének felelős és hatékony szervezése és ellenőrzése érdekében. Az HSBC Insurance Brokers ügy azért is érdekes, mert itt az üzleti gyakorlattal kapcsolatos mulasztás alapján szabtak ki bírságot, nem pedig a személyes adatok tényleges sérelme miatt.[33]

- Ugyancsak az Egyesült Királyságban, a jelzálog és lakossági banki szolgáltatásokat nyújtó Nationwide Building Society-t 980.000 GBP-re bírságolták egy munkavállaló ügyféladatokat tartalmazó laptopjának ellopását követően. Az FSA véleménye szerint a Nationwide biztonsági rendszere és az adatbiztonsági eseményre adott válasza nem volt megfelelő.[34]
- 2009-ben az ICO egy mobilszolgáltatónál végzett ellenőrzést, miután felmerült a gyanú, hogy a társaság munkavállalói ügyfelek mobiltelefon szerződéseit, beleértve a szerződések lejártával kapcsolatos adatokat kínáltak eladásra. Az információkat állítólag a versenytársaknak értékesítették, amelyek ügynökei azokat arra használták, hogy az ügyfeleket hideg hívással (*cold call*) felkeressék a szerződésük lejártát megelőzően más szolgáltatásokat felkínálva. Állítólag több ezer ügyfél számlaadatai kerültek ki jogosulatlanul.[35]
- 2009 végén az HSBC svájci private banking üzletágának 15.000 számlájából egy munkavállaló állítólag adatokat lopott, amelyek végül a francia, illetve az olasz hatóságok kezébe kerültek, akik ezt felhasználva majdnem 3.000 személy ellen kezdtek vizsgálatot, adóelkerülés és pénzmosás kapcsán.[36]
- Az ICO 2011 februárjában 80.000, illetve 70.000 fontra bírságolta az Ealing Council-t és Hounslow Council-t, mert az adatkezelők két, nem titkosított adatokat tartalmazó

---

33 Lásd Simon Hunt biztonsági szakértő véleményét: **FSA fines HSBC companies $7,500,000 for data security issues** http://siblog.mcafee.com/data-protection/fsa-fines-hsbc-companies-7500000-for-data-security-issues/ és HSBC Gets Record **Fine for Data Breach, Security VARs 'Bank' on Continuing Trend** http://www.itbusinessedge.com/cm/blogs/bentley/hsbc-gets-record-fine-for-data-breach-security-vars-bank-on-continuing-trend/?cs=34398

34 **FSA fines Nationwide £980,000 for information security lapses** http://www.fsa.gov.uk/pages/Library/Communication/PR/2007/021.shtml

35 **T-Mobile says staff sold phone records to rivals** http://www.out-law.com/page-10531

36 **HSBC: Data theft incident broader than first thought** http://www.computerworld.com/s/article/9169218/HSBC_Data_theft_incident_broader_than_first_thought

laptopját ellopták.[37]

- Az ICO 2011. június 9-én 120.000 fontra bírságolta a Surrey County Council-t, mert három alkalommal nem megfelelő címzettek számára küldött el e-mailben különleges adatokat (pl. 241 személy egészségügyi adatait).[38]
- 2011 augusztusában egy ingatlanos cég munkatársa vesztett el egy 26.000 ügyfél személyes adatait tartalmazó pendrive-ot – egy angol pub-ban.[39]
- Az egészségügyi szektorban szintén akad példa adatbiztonsági eseményre Európában is. Az ír adatvédelmi hatóság 2011 augusztusában egy, az USA-ban működő szolgáltató hatvan ügyfelének (köztük négy kórháznak) küldött adatbiztonsági értesítést, mert az érintett szolgáltatóval kapcsolatban a páciensek adatai jogtalan értékesítésének gyanúja merült fel. Egyes érintett ügyfelek arról sem tudtak, hogy a szolgáltató tulajdonosi köre többször megváltozott – az ilyen jellegű adatfeldolgozási viszony esetén ezért is lehet szükség az adatfeldolgozó tulajdonosi körének megváltozását a szerződő partnerek előzetes beleegyezéséhez, vagy legalább értesítéséhez kötni (*change control*).[40]
- A közösségi oldalak ugyancsak kedvelt célpontjai a hackereknek. Németországban például a StudiVZ közösségi honlap jelszavait és e-mail címeit lopták el[41], de a Facebook körül is időről-időre felmerülnek adatbiztonsági események, például az egyes alkalmazásokon keresztül véletlenül továbbított személyes adatokkal kapcsolatban.[42]
- A gyermekek adatai szintén veszélyeztetettek: az ICO azért marasztalta el a Scottish Children's Reporter Administration (SCRA) nevű gyermekvédő szervezetet, mert egy kiselejtezett és használtbútor-kereskedésben továbbértékesített szekrényben gyermekek személyes adatait tartalmazó belső anyagokat felejtettek. Később ugyanez a szervezet küldött véletlenül rossz e-mail címre egy folyamatban levő bírósági eljárással kapcsolatos, az ügyben vizsgált gyermekbántalmazás részletes leírását és az

---

37 **Councils fined for unencrypted laptop theft** http://www.ico.gov.uk/~/media/documents/pressreleases/2011/Monetary_penalties_ealing_and_hounslow_news_release_20110208.ashx+Ealing+Council+ico&ct=clnk

38 **ICO fines Surrey county council for data breaches** http://www.guardian.co.uk/government-computing-network/2011/jun/09/surrey-data-protection-breach-information-commissioner-s-office-fine

39 **DOH! Housing contractor loses unencrypted stick down the pub** http://www.topsession.net/magazine/2322-doh-housing-contractor-loses-unencrypted-stick-down-the-pub

40 **Irish Data Breach Could Touch United States** http://www.healthdatamanagement.com/news/data-breach-ireland-irish-notification-43022-1.html

41 **Daten-Gau bei StudiVZ** http://www.focus.de/digital/internet/online-community_aid_125470.html

42 **Facebook trashes Symantec report on data breach** http://www.ibtimes.com/articles/144400/20110512/facebook-symantec-data-breach-access-token-privacy-security-advertisers-deny.htm **Facebook admits 'inadvertent' privacy breach** http://www.telegraph.co.uk/technology/facebook/8070513/Facebook-admits-inadvertent-privacy-breach.html

érintettek személyes adatait tartalmazó anyagot. Az ICO-t az esetekkel összefüggésben az a kritika érte, hogy nem szabott ki pénzbírságot az adatkezelőre, csak kötelezte, hogy tartson oktatást munkavállalóinak a belső adatvédelmi szabályzatáról és ellenőrizze annak betartását.[43]

Adatbiztonsági eseményekre **Magyarországon** is akad példa.

- A kormányzati portálnál merült fel kétszer is adatbiztonsági esemény. 2009 februárjában egy biztonsági hiba miatt emberek ezreinek lett hozzáférése az Adó-és Pénzügyi Ellenőrzési Hivatal és más személyek, illetve társaságok közötti levelezésekhez. A levelezések magánszemélyek adóbevallásait és adóazonosítóit is tartalmazhatták volna. Habár az esemény nem volt jelentős, mert a személyes adatok csak véletlenszerűen tűntek fel és adott nevekre nem tudtak a felhasználók rákeresni, az Adatvédelmi Biztos az érintett biztonsági eljárásoknak a rendszer jogi és technikai feltételeivel együtt történő átfogó vizsgálatát rendelte el.[44] 2010 márciusában egy kevésbé súlyos eseményre került sor (amelyet azonnal orvosoltak): az adott időszakban bejelentkezett felhasználók mintegy tizedénél nem jelent meg visszaigazolás, továbbá körülbelül két százalékuk véletlenszerűen másnak szóló visszaigazolásokat láthatott, ugyanakkor állítólag ezek a visszaigazolások nem tartalmaztak bizalmas információkat és csupán 24 felhasználó volt érintett. Ebben az esetben is az Adatvédelmi Biztos vizsgálta az ügyet, különösen a rendszer adatbiztonságának tesztelési módszereit és a szolgáltatás hiányát, valamint azt is megjegyezte, hogy a személyes adatok helytelen „összekeverése" és véletlen közzététele kifogásolható még akkor is, ha a személyes adatokkal nem éltek vissza.[45]
- Egy másik jelentős adatbiztonsági esemény szintén az állami szférában történt: 2008-ban egy adminisztrátor hanyagsága eredményeképpen 1.717 egyetemi hallgató személyes adata (pl. neve, az egyetemi rendszerhez tartozó jelszava, e-mail címe, címe, bankszámlaszáma) 2,5 hónapon keresztül nyilvánosan elérhetővé vált az interneten keresztül. Az érintett diákokat értesítették, hogy azonnal intézkedjenek a

[43] **ICO left fuming as children's case files turn up in second-hand furniture shop** http://www.v3.co.uk/v3-uk/news/2106317/ico-left-fuming-childrens-files-hand-furniture-shop

[44] **Az adatvédelmi biztos az Ügyfélkapu hétvégi hibájáról** http://abiweb.obh.hu/abi/index.php?menu=0/Sajtokozlemenyek&dok=20090209_ABI_1

[45] **Vizsgálja az adatvédelmi biztos az Ügyfélkapu üzemzavarát** http://abiweb.obh.hu/abi/index.php?menu=0/Sajtokozlemenyek&dok=20100311_ABI_1

jelszavaik megváltoztatása érdekében.[46]

## 6. Az adatgazdák (ügyfelek) tipikus panaszai az adatbiztonsági eseményekkel kapcsolatban

Az USA-ban az első adatbiztonsági eseményről szóló értesítésekre vonatkozó szabályok elfogadása óta számos, vállalkozásoknál, állami szerveknél és oktatási intézménynél bekövetkező adatbiztonsági eseményt jelentettek. Ebben a pontban példálódzó jelleggel felsoroljuk az érintett adatgazdák által érvényesített követelések és panaszok jellegét. Fontos tudni, hogy a leggyakrabban az ilyen jellegű kereseteket elutasítják, egyrészt mert az adatbiztonsági eseményekkel kapcsolatos, az adatgazdák oldalán jelentkező veszteségek csak nagyon ritkán számszerűsíthetők, másrészt a bíróságok a személyiséglopás által okozott érzelmi károkat általában nem, csak a gazdasági veszteségeket állapítják meg. A fent említett „*JetBlue*" esetben például az ügyfelek keresetei az állítólagos gazdasági károk hiányában elutasításra kerültek és a bíróság megjegyezte, hogy az ügyfelek nem várhatnak el egyébként kompenzációt a személyes adataik értéke alapján.

- **Az adatkezelő gondatlansága**

Az úgynevezett „*Providence*" ügyben az illetékes michigani bíróság megállapította az adatkezelő gondatlanságát, mert az nem biztosította a nyilvántartásai biztonságos helyen történő őrzését (pl. adatok hazavitele, titkosítás elmulasztása, biztonsági másolatok készítésének elmulasztása), és indokolatlanul késlekedett az ügyfelek adatlopásról való értesítésével (és ezáltal az ellopott információval való esetleges visszaélés megelőzésével).[47]

Az említett esetben az adatkezelő szervezet pénztárosa olyan iratokat vitt haza, amelyek a szervezet tagjainak nevét és társadalombiztosítási számát tartalmazta. Az esküdtszék megállapította, hogy a pénztáros lánya ellopta az információkat és arra használta fel őket, hogy a tizenhárom szervezeti taggal szemben (felperesek) személyiséglopást kövessen el, ugyanakkor az adatkezelő gondatlanul elmulasztotta a megfelelő biztonsági intézkedések megtételét személyes adatok ellopása ellen. Az adatkezelő kötelezettsége, hogy biztosítsa tagjai személyes adatainak védelmét, mert a tagokhoz képest hatékonyabban tudja ellenőrizni a személyiséglopáshoz felhasznált személyes adatokhoz való hozzáférést, és megnövekedett mértékű személyiséglopások által jelentett fenyegetettség miatt a nem

[46] **Ezerhétszáz hallgató adatait vesztette el a veszprémi egyetem** http://www.origo.hu/techbazis/internet/20081210-1717-hallgato-adatait-vesztette-el-a-veszpremi-egyetem.html

[47] Részletesen elemzi: **Anita Ramasastry: Data Insecurity: What Remedy Should Consumers Have When Companies Do Not Keep Their Data Safe?** http://writ.news.findlaw.com/ramasastry/20060306.html

biztonságos környezetben tárolt különleges adatokkal kapcsolatos kockázat is előrelátható volt. A felmerülő károk mértéke ugyancsak felmérhető, mivel a személyiséglopás jelentős mértékű pénzügyi veszteségeket és károkat okozhat például az érintett személlyel kapcsolatos – az USA-ban napi szinten használt – hitelinformációk szempontjából. A társadalombiztosítási számokkal való visszaélés és az adatkezelő felelőssége megállapításának következtében az illetékes bíróság 275.000 USD megfizetését írta elő az adatkezelő számára. [48]

Egy másik esetben egy Tennessee-i bíróság megállapította az MBNA America Bank felelősségét egy személyiséglopást elszenvedett személy kára tekintetében: az érintett személy gyenge hitelminősítése miatt nem kapott meg egy állást, ugyanakkor a személyiséglopást követően az MBNA gondatlanul elmulasztotta az ügy kivizsgálását, beleértve az áldozat hitelkérelmében szereplő hitelinformációk pontosságának igazolását.[49]

- **Az érintett személyek késedelmes értesítése**

A „*Providence Healthcare Systems*" ügyben az érintett páciensek kifogásolták, hogy csak egy hónappal az eset bekövetkezését követően értesítették őket az adatbiztonsági eseményről. A sértett felek hasonló panasszal éltek a „*Veterans Administration*" ügyben: a Veterans Administration legalább héttel az adatbiztonsági esemény bekövetkezése után tájékoztatta a nyilvánosságot arról, hogy veteránok millióinak neve, társadalombiztosítási száma és születési dátuma jutott illetéktelenek tudomására. Ezt követően a társaság további két hetet várt annak beismerésével, hogy a lopás nagyszámú aktív személy nyilvántartására is kiterjedhet.[50]

- **Az adatkezelés felfüggesztése**

A Veterans Administration adatbiztonsági eseménye kapcsán a sértett személyek kérelmezték a bíróságtól, hogy tiltsa el a Veterans Administration munkavállalóit a különleges adatok használatától mindaddig, amíg egy független szakértő meg nem állapítja, hogy a Veterans Administration megfelelő védelmet biztosít a kérdéses adatoknak.

---

[48] Bell v. Michigan Council 25 AFSCME http://library.findlaw.com/2005/May/19/174549.html

[49] Wolfe v. MBNA America Bank, No. 05-2972 (W.D. Tenn. 04/25/07) http://ephemerallaw.blogspot.com/2007/06/court-holds-bank-liable-for-failure-to.html

[50] Részletesen elemzi Anita Ramasastry: **Stolen Laptops and Data Theft** http://writ.news.findlaw.com/ramasastry/20060615.html

- **Az adatgazdák érzelmi kárai**

A felperesek – pl. az „*Amburgy v. Express Scripts*" ügyben[51] – olyan érzelmi károkért is kártérítést kérhetnek, amelyek a jövőbeli személyiséglopástól való félelemből, a veszteségek elkerülése érdekében folytatott hitelfigyeléssel (*credit monitoring*) kapcsolatosan felmerült költségekből erednek. Az ilyen jellegű károk felmérésére egyébként már külön pszichológia kutatásokat is végeznek.[52]

- **Az adatgazdák megtévesztése**

A sérelmet szenvedett felek az adatbiztonsági intézkedésekkel kapcsolatos félretájékoztatás miatt is perelhetnek társaságokat, amint ez az úgynevezett „*Pinero*" ügyben is történt.[53] A felperes, Vicki Pinero adóbevallásának elkészítésével bízott meg egy társaságot, és a társaság az adóbevallással kapcsolatos, már szükségtelen dokumentumokat egy utcai kukába dobta, ahol egy járókelő megtalálta azokat. Az adóbevallások nem kerültek megsemmisítésre, és a vonatkozó jogszabályok szerint sem tették azokat egyéb módon olvashatatlanná. A társaság adatvédelmi szabályzatának rendelkezései szerint ugyanakkor megfelelő (fizikai, elektronikus és egyéb) eljárások kerültek bevezetésre az ügyfelek személyes adatai védelme érdekében: a felperes Pinero állítása szerint ő ebben az állításra hagyatkozva bízta meg a társaságot és adta át számára személyes adatait.

## 7. Az adatbiztonsági értesítésekkel kapcsolatos jogalkotás és az EU szabályozásának legsúlyosabb hiányosságai

A személyes adatok védelme jelenleg a világon mindenhol kulcskérdés. A személyes adatokat tartalmazó adatbázisok elleni támadások számának folyamatos növekedésére válaszul, valamint az adatbiztonsági eseményekkel kapcsolatos kockázatok enyhítése érdekében az első specifikus jogszabályt 2003-ban alkották meg Kaliforniában, és hamarosan az USA többi tagállama is hasonló, nagyon részletes és szigorú kötelezettségeket megállapító jogszabályokat fogadott el.

---

[51] Az ügy teljes körű elemzése a következő cikkben: **Anita Ramasastry: A Federal Court Dismisses a Suit Based on a Threat of Identity Theft and an Extortion Letter** http://writ.news.findlaw.com/ramasastry/20100127.html

[52] **Identity Theft Has Long Lasting Psychological Effects** https://infosecisland.com/blogview/15962-Identity-Theft-Has-Long-Lasting-Psychological-Effects.html

[53] Az ügy teljes körű elemzése a következő cikkben: **Anita Ramasastry: A Court Holds that When a Company Breaks Its Promise to Keep Information Safe, It Cannot Be Sued: The Right Result, but One that Suggests the Need to Change the Law?** http://writ.news.findlaw.com/ramasastry/20090130.html

Az adatbiztonsági értesítésekre vonatkozó szabályozás EU szintű bevezetésére az e-Privacy Irányelv módosításával került sor. A vonatkozó módosításokat a tagállamoknak 2011. május 25-ig kellett átültetniük – Magyarországon az adatbiztonsági értesítésekre vonatkozó rendelkezések az elektronikus hírközlésről szóló 2003. évi C. törvény (**„Eht."**) 156. §-ba kerültek be.[54] Fontos megemlíteni, hogy az Európai Parlament és a Tanács 2002. március 7-i - az elektronikus hírközlő hálózatok és elektronikus hírközlési szolgáltatások közös keretszabályozásáról szóló - 2002/21/EK irányelvének (**„Keretirányelv"**) módosítása[55] is bevezetett néhány általános, IT biztonsági értesítési kötelezettséget.

Az új szabályozás azonban mind összetettségét, mind tárgyi hatályát tekintve sajnos elmarad az elvárható jogalkotási iránytól és gyakorlati igényektől, különös tekintettel a fent ismertetésre került amerikai szabályozástól. Az adatvédelmi szabályozására hagyományos büszke EU egyelőre jelentős lemaradásba került a ma talán legfontosabb adatvédelmi-szabályozási kérdésben. Megállapítható, hogy az adatbiztonsági értesítésekkel kapcsolatos feladatok szempontjából ma az USA szabályozása az európainál messze fejlettebb, gyakorlatiasabb és naprakészebb: ugyanakkor a napi szintű globális adatáramlások világában az iparági követelmények és az adatgazdák védelme miatt az EU számára is létfontosságú, hogy a jogalkotás területén mielőbb felzárkózzon az USA-hoz, valamint lépést tartson az iparági- és ügyfélelvárásokkal. Különösen szükség lehet specifikus értesítési kötelezettségekre azokban az iparágakban, ahol az átlagosnál nagyobb az adatvesztés, személyiséglopás vagy akár pénzügyi veszteség kockázata: közösségi oldalak, online tranzakciók, e-banking szolgáltatások, e-health szolgáltatások.[56]

Az EU szabályozás legnagyobb hiányosságai a következők:

- **Indokolatlanul szűk hatály**

Az értesítési előírások kizárólag az elektronikus hírközlési szektorra korlátozódnak, pedig a más iparágakban személyes adatokat rendelkezésre bocsátó adatgazdáknak is az az érdeke, hogy az adatbiztonsági események hátrányos következményeinek és az általuk okozott anyagi kár elkerülése

[54] A jogalkotási folyamatról részletesen ld. Bíró János - Szádeczky Tamás – Szőke Gergely László: **A hírközlési szolgáltatók értesítési kötelezettsége a személyes adatok megsértése esetén** (Infokommunikáció és Jog 43. szám, 2011. április)

[55] 2009/140/EK Irányelv

[56] **Commission considers wider-ranging data breach notification law** http://www.out-law.com/page-10480

érdekében értesítést kapjanak az adatbiztonsági eseményekről. A tájékoztatási kötelezettség tehát nem korlátozható az elektronikus hírközlési szektorra: kötelező jellegű adatbiztonsági értesítési előírások alkalmazására lenne szükség valamennyi iparágban, európai szinten.[57]

Az EU adatbiztonsági értesítésekkel kapcsolatos szabályozásával és annak lehetséges jövőben irányával kapcsolatban a 29. Cikk Munkacsoport (amely az Adatvédelmi Irányelv alapján működő, a tagállamok nemzeti adatvédelmi felügyelő hatóságainak vezetőiből, biztosaiból álló, a Bizottság mellett működő független tanácsadó szerv) is hasonló véleményen van – észrevételeiket a 01/2011. számú véleményük tartalmazza.[58]

Az adatbiztonsági értesítési kötelezettség egyéb iparágakra való kiterjesztését maga az e-Privacy Irányelvet Módosító Irányelv is rögzíti, miszerint *„a biztonság megsértésére vonatkozóan nyújtott tájékoztatás a polgárok azon általános érdekét tükrözi, hogy tájékoztatást kapjanak a biztonsági rendszer olyan hibáiról, amelyek következtében személyes adataik elveszhetnek vagy egyéb módon veszélybe kerülhetnek, illetve azokról a rendelkezésre álló vagy javasolt elővigyázatossági eszközökről, amelyek segítségével minimálisra csökkenthető az ilyen hibákból eredő esetleges gazdasági veszteség vagy társadalmi kár. A felhasználóknak ez a tájékoztatásra vonatkozó általános érdeke egyáltalán nem korlátozódik az elektronikus hírközlési ágazatra, éppen ezért közösségi szinten kiemelkedő fontosságúnak kell tekinteni a kifejezett, kötelező és minden ágazatra és az információs társadalommal összefüggő szolgáltatások szolgáltatóira kiterjedő tájékoztatási kötelezettség szükségességét is ideértve. Az e területre vonatkozó európai jogszabályok Bizottság általi felülvizsgálatáig a Bizottságnak - az európai adatvédelmi biztossal konzultálva - haladéktalanul meg kell tennie a megfelelő lépéseket a 2002/58/EK irányelv (elektronikus hírközlési adatvédelmi irányelv) által meghatározott, az adatok megsértésére vonatkozó tájékoztatási kötelezettség keretében megfogalmazott elveknek más ágazatokban történő alkalmazásának lehetőségeiről, az ágazattól, illetve az érintett adat jellegétől függetlenül.”* [59]

A Bizottságnak a személyes adatok Európai Unión belüli védelmének átfogó megközelítéséről szóló közleménye szintén rögzíti, hogy *„mivel más ágazatokban (pl.: a pénzügyi szektorban) is fennáll az adatsértés veszélye, a Bizottság megvizsgálja, hogy milyen módon terjeszthető ki egyéb ágazatokra a személyes adatok megsértésére vonatkozó bejelentési kötelezettség”*[60]

---

57 **European Commission passes new E-Privacy Directive requiring mandatory data breach notification by public communications providers** http://www.lexology.com/library/detail.aspx?g=c3d22861-a43c-4cd0-9294-b89664984101

58 **Working Document 01/2011 on the current EU personal data breach framework and recommendations for future policy developments** http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp184_en.pdf

59 Módosító Irányelv, Preambulum (59)

60 **A Bizottságnak a személyes adatok Európai Unión belüli védelmének átfogó megközelítéséről szóló közleménye** http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_hu.pdf

Egyes országokban az adatvédelmi hatóságok szerencsére már vizsgálják, hogy milyen módosítások szükségesek a tagállami adatvédelmi jogszabályokban egy általános, iparág-független adatbiztonsági értesítési kötelezettség bevezetése érdekében. Írországban például az adatvédelmi biztos (*Data Protection Commissioner*) 2009 áprilisában már útmutatást is kibocsátott az adatbiztonsági értesítési eljárások lefolytatásával kapcsolatban – lényege, hogy ha egy adatkezelő észleli az érdekkörébe tartozó személyes adatok biztonságának megsértését, haladéktalanul értesítse az adatvédelmi biztost.[61] Ausztriában[62] és Németországban[63] az adatbiztonsági értesítési kötelezettségeket más iparágakra is kiterjesztették, és a világon máshol is ez a tendencia - legutóbb például Új-Zélandon javasolta a jogalkotó ugyanezt (egyébként egy figyelemre méltóan terjedelmes, 162 oldalas adatvédelmi reformjavaslat részeként)[64]. Olaszországban az illetékes hatóság (*Garante*) 2011. június 3.-án hasonló – adatbiztonsági értesítési eljárásokkal és adatbiztonsági intézkedésekkel kapcsolatos - ajánlást bocsátott ki bankok számára.[65]

- **Túl általános rendelkezések**

Az e-Privacy Irányelv új rendelkezései csak nagyon általános szinten fogalmazzák meg az adatbiztonsági értesítésekkel kapcsolatos szabályokat. Elengedhetetlen tehát, hogy a tagállami jogalkotók, illetve szabályozó hatóságok mielőbb kibocsássák részletes iránymutatásaikat a témában és az adatkezelőkkel együttműködve (például nyilvános konzultációk során) segítsék azok gyakorlati alkalmazását. A módosított E-Privacy Irányelv alapján elfogadott tagállami szabályozásoknak az USA-beli szabályozáshoz hasonlóan például a gyakorlatban is működőképes fogalom-meghatározásokat kellene tartalmazniuk az adatbiztonsági események kapcsán.

- **Felkészülési idő hiánya**

Az e-Privacy Irányelv implementációját követő kezdeti időkre egfontolandó lehet „türelmi idő" biztosítása az adatkezelők számára, vagyis az adatbiztonsági értesítési kötelezettségek nem

61 **Data Protection Commissioner issues Guidance on Data Breaches** http://dataprotection.ie/viewdoc.asp?Docid=913&Catid=75&StartDate=01+January+2009&m=n

62 **Datenschutzgesetz 2000** https://www.dsk.gv.at/DocView.axd?CobId=40904

63 **Bundesdatenschutzgesetz** http://www.bfdi.bund.de/EN/DataProtectionActs/Artikel/BDSG_idFv01092009.pdf?__blob=publicationFile

64 http://www.lawcom.govt.nz/sites/default/files/publications/2011/08/web_pdf2_review-of-the-privacy-act-1993-webpdf-72dpi-chapter-7-appendix_1.pdf

65 **Italy: Garante recommends banks notify customers of data breaches** http://www.dataguidance.com/news.asp?id=1535

rosszhiszemű (hanem például a nem egyértelmű szabályozásból eredő) megszegése esetén az illetékes hatóság egy bizonyos ideig ne szankcionálja az adatkezelőt.

- **Preventív jellegű szabályozás**

További probléma, hogy az európai általános adatbiztonsági szabályok általánosságban preventív jellegűek, és az érintettek előzetes tájékoztatására épülnek, ugyanakkor kevésbé fókuszálnak egy-egy adatbiztonsági esemény utáni teendőre.

- **Határon átnyúló adatkezelések szabályozatlansága**

Az e-Privacy Irányelv nem kezeli megfelelően a több országot érintő adatbiztonsági eseményeket sem. Ahogy az USA esetében is, az Európai Unióban is nagyon sok adatkezelő végez határokon átnyúló tevékenységet, ezért EU-s szintű, az E-Privacy Irányelv követelményeivel összhangban álló, ugyanakkor a meglévő keretszabályoknál jóval specifikusabb adatbiztonsági értesítési részletszabályozás szükséges. A jogszabályoknak való gyakorlati megfelelés érdekében a tagállami adatvédelmi hatóságoknak megfelelő végrehajtási eszközöket kell biztosítani.

Az EU szabályozás hiányosságai részletesen a következő fejezetben kerülnek kifejtésre.

## II. AZ ADATBIZTONSÁGI ÉRTESÍTÉSEKKEL KAPCSOLATOS SZABÁLYOK AZ USA TAGÁLLAMI JOGSZABÁLYAIBAN ÉS AZ E-PRIVACY IRÁNYELVBEN

Amint az már fent említésre került, az első adatbiztonsági értesítésekkel kapcsolatos jogszabályt Kaliforniában fogadták el. Az USA többi tagállamának hasonló jogszabálya általában a (nemrég módosított[66]) kaliforniai jogszabály alapján készült, ezért a jelen fejezet is ezt, valamint a szintén figyelemreméltó, minden részletszabályra kiterjedő floridai megfelelőjét veszi alapul. Az európai jogi háttérre való hivatkozás vagy az EU általános „Adatvédelmi Irányelvére”[67] szóló irányelvre, vagy a (módosított) e-Privacy Irányelvre történik.

[66] **State Senate Passes Amendments to CA Breach Notification Law** http://www.insideprivacy.com/united-states/state-senate-passes-amendments-to-california-breach-notification-law/

[67] Az Európai Parlament és a Tanács 95/46/EK irányelve (1995. október 24.) a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról

## 1. Adatbiztonsági értesítések – általános rendelkezések

### 1.1 Értesítési kötelezettségek "saját" adatokkal kapcsolatban

Az USA legtöbb tagállamában az adatkezelő „saját" adataival kapcsolatos adatbiztonsági eseményekről való értesítéssel összefüggő általános kötelezettségek szabályozása nagyjából hasonló. Bármely személy, aki egy adott tagállam területén üzleti tevékenységet végez és személyes adatokat is tartalmazó információt kezel, az adatbiztonsági esemény azonosítását követően köteles értesíteni a tagállamnak azt a lakosát, akinek a nem titkosított személyes adatához valószínűsíthetően vagy ténylegesen illetéktelen személy jutott hozzá. Az értesítést a lehető leghamarabb és ésszerű késedelem nélkül, a bűnügyi hatóságok jogszerű érdekeire, valamint az adatbiztonsági esemény részleteinek megállapításához és az érintett (adatkezelési) rendszer egysége visszaállításához szükséges intézkedésekre figyelemmel kell megtenni.[68]

A vonatkozó jogszabály az értesítés megtételére meghatározott időtartamot is előírhat – ez a leggyakrabban 45 nap.

Számos tagállam (pl. Washington[69], New York[70] és Kalifornia[71]) jogszabálya külön kezeli a „saját" és a „felhatalmazás" alapján kezelt (feldolgozott) személyes adatokat. A kaliforniai jogszabály azt is tisztázza, hogy a „saját" és a „felhatalmazás" alapján kezelt (feldolgozott) személyes adatok többek között magukban foglalják az adatkezelő ügyfelei és szerződő felei személyes adatait is.[72]

*Az e-Privacy Irányelv rendelkezései:*

Az adatbiztonsági eseményre vonatkozó bejelentési kötelezettségeket az e-Privacy Irányelv szerint a következő személyek irányában kell teljesíteni:

- **Az illetékes nemzeti hatóság értesítése.** A személyes adatok megsértése esetén a nyilvánosan elérhető elektronikus hírközlési szolgáltatást nyújtó illetékes szolgáltató indokolatlan késedelem nélkül bejelenti az illetékes nemzeti hatóságnak a személyes

68 1798.82. (a) (Cal. Civ. Code)
69 Wash. Rev. Code §19.255.010 (1)
70 N.Y. Gen. Bus. Law § 899 §-aa
71 1798.82. (a) (Cal. Civ. Code)
72 1798.81.5. (a) (Cal. Civ. Code)

adatok megsértését.[73]

- **Az érintett személyek értesítése.** Ha a személyes adatok megsértése várhatóan hátrányosan érinti az előfizető vagy magánszemély személyes adatait vagy magánéletét, akkor a szolgáltató erről az előfizetőt vagy magánszemélyt is indokolatlan késedelem nélkül értesíti.[74]A „hátrányosan érinti" kifejezés sajnos nem került bővebben meghatározásra a módosított E-Privacy Irányelvben, ugyanakkor a Módosító Irányelv Preambuluma iránymutatásul szolgálhat. E szerint „*egy biztonsági esemény akkor jelent az előfizető személyes adataira vagy magánéletére nézve súlyos veszélyt, ha például személyazonossággal való visszaélést, fizikai kárt, durva sértést vagy hírnévrontást von maga után a Közösségben a nyilvánosan elérhető hírközlési szolgáltatások nyilvános hírközlő hálózaton történő nyújtásával összefüggésben*".[75]

*Megfontolásra érdemes kérdések az e-Privacy Irányelv implementációja során:*

- Fontos kérdés a címzettek körének meghatározása. Indokolt egyrészről az „első számú" címzettként az illetékes hatóságot meghatározni, annak érdekében, hogy az adatkezelő az adatgazdákat ne terhelje feleslegesen a kevésbé jelentős vagy már el is hárított veszélyekről szóló értesítésekkel. Az európai szabályozás szerint azonban felmerülhet egy olyan probléma, hogy ha a hatóság mégis indokoltnak tartja az adatgazdák értesítését, a hatóság vizsgálatának ideje alatt az adatgazdák érdekei esetleg már sérültek, hiszen nem tudtak az adatbiztonsági eseményről, és nem is tudtak semmilyen óvintézkedést tenni. Ilyen esetben egy-két nap késedelem is súlyos károkat okozhat. Fontos tehát, hogy az illetékes hatóságokra megfelelő és specifikus határidők legyenek irányadók annak elbírálása során, hogy szükséges-e az adatgazdák közvetlen értesítése. Az érintettek közvetlen értesítési kötelezettségének bevezetése mellett ugyancsak vannak érvek, hiszen az adatbiztonsági események számának várható növekedésével párhuzamosan a tagállami illetékes hatóságoknak nem feltétlenül áll majd rendelkezésre megfelelő erőforrás a kapcsolódó felügyeleti feladatok ellátásához, és mire az adott hatóság elbírálja, hogy szükséges-e az érintett személyek közvetlen értesítése, a személyes adatokkal való visszaélés esetleg már be is következhet.

[73] e-Privacy Irányelv 4. cikk (3)
[74] e-Privacy Irányelv 4. cikk (3)
[75] Módosító Irányelv (61) preambulum-bekezdése

- Érdemes lehet azt is tisztázni, hogy az érintettek közvetlen értesítése esetén adatbiztonsági szempontból elegendő-e csak a „közvetlenül" érintett személyek (például: az adatgazda munkavállalók) értesítése, vagy szükséges-e az eseményről a lehetséges „közvetett" érintettek (például a közvetlenül értesített „adatgazda" munkavállalók e-mail kontaktszemélyeinek) értesítése.
- A gyakorlatban különösen hasznos, hogy az amerikai szabályozás kifejezett külön kezeli a „saját" és a „felhatalmazás alapján kezelt" adatokat. A nem jogász adatkezelők ugyanis nem feltétlenül ismerik fel a „saját" (pl. munkavállalók, szerződőpartnerek adatai) és a „felhatalmazás" alapján kezelt (feldolgozott) adatok megítélése közötti jogi különbséget. Egy adatbiztonsági esemény esetén ugyanakkor nagyon fontos, hogy az adatkezelő mielőbb azonosítsa az érintett adatokat és személyeket, valamint a rá irányadó értesítési és biztonsági kötelezettségeket.
- Az e-Privacy Irányelvben az „*indokolatlan késedelem nélkül*" kifejezés nem került meghatározásra. Ismét a Módosító Irányelv preambuluma szolgálhat iránymutatásul: eszerint a nyilvánosan elérhető hírközlési szolgáltatónak a biztonság megsértéséről a nemzeti szabályozó hatóságot „*a biztonság megsértéséről való értesülését követően azonnal*" értesítenie kell. [76] Jelenleg tehát az EU-ban nincs egységes, specifikus határidő az értesítési kötelezettség teljesítésére. Az adatbiztonsági eseményt követően azonban az adatkezelőnek ésszerű – általában pár napos - időre van szüksége arra, hogy felmérje az esemény pontos körülményeit, megfogalmazza az értesítés tartalmát és közben megtegye a halasztást nem tűrő biztonsági intézkedéseket is. Ennek érdekében a tagállami szabályozásokban pontosan rögzíteni kellene, hogy az „indokolatlan késedelem" nélküli eljárás során pontosan milyen intézkedésekre van idő, és legalább hozzávetőlegesen mik az irányadó (specifikus) határidők.
- Felmerül a kérdés a gyakorlatban, hogy milyen kötelezettségek vonatkozhatnak azokra a társaságokra, akik ugyan személyes adatot nem, de egyéb szenzitív információt – üzleti titkokat (szellemi alkotások, kutatási anyagok, pénzügyi iratok) – kezelnek, és az ilyen információk biztonsága kerül veszélybe. A jelenlegi jogalkotási tendencia szerint egyelőre az adatbiztonsági értesítési kötelezettségek ezeket az információkat nem érintik, pedig akár ez is indokolt lehet.

[76] Módosító Irányelv (61) preambulum-bekezdése

### 1.2 Előzetes vizsgálatok

Az USA-ban az arizonai jogszabály szerint a fentihez hasonló értesítési kötelezettség mellett az adatkezelő az értesítést megelőzően vizsgálatot köteles végezni annak megállapítására, hogy valóban történt-e az adott rendszerrel kapcsolatban adatbiztonsági esemény.[77] Maine állam jogszabálya azt is előírja, hogy a gyorsan, ésszerűen és jóhiszeműen lefolytatott vizsgálat célja azt is megállapítani, hogy a személyes adatokkal visszaéltek-e, vagy visszaélhetnek-e.[78]

A vizsgálatra nem csak azért lehet szükség, mert a vonatkozó jogszabály előírja, hanem az adatkezelő saját érdekében is: az adatbiztonsági esemény sikeres kivizsgálása elősegítheti az adott esemény bekövetkezéséig esetleg nem ismert kockázat azonosítását, valamint segítheti a vonatkozó belső eljárásoknak a kockázat elhárítása érdekében való felülvizsgálatát.

A vizsgálatba ugyanakkor harmadik személyek bevonása is szükséges lehet. Ez történt, amikor a Wyoming állam-béli Rocky Mountain Bank pert indított a Google ellen, hogy fedje fel egy Gmail felhasználó személyazonosságát, miután a bank egyik alkalmazottja a felhasználó számára véletlenül elküldte a bank mintegy 1.300 ügyfelének a nevét, címét, adószámát és hitelviszonyukkal kapcsolatos adatoka.[79] Figyelembe véve, hogy az érintett harmadik fél – ebben az esetben a Google – a kért személyes adat visszatartására megfelelő jogalappal rendelkezhet, és a kérésnek csak jogerős bírósági vagy hatósági felszólítás esetén köteles eleget tenni, a vizsgálat aránytalanul hosszú időt vehet igénybe, és ez ésszerűtlen ráfordításokat és költségeket jelenthet az adatkezelő számára, valamint az érintett adatgazdák bizalomvesztéséhez is vezethet.

*Megfontolásra érdemes kérdés az e-Privacy Irányelv implementációja során:*

- Az e-Privacy Irányelv nem tartalmaz a fentiekhez hasonló kifejezett előzetes vizsgálati kötelezettséget. Tekintettel arra azonban, hogy az adatbiztonsági értesítési eljárások az EU-ban még ritkábbak, és kevésbé alakult ki a gyakorlatuk, érdemes lehet részletesebben leírni az adatkezelők számára, miként kell az esemény vizsgálatát elvégezni, mire kell, hogy a vizsgálat kiterjedjen. A vizsgálat célja nem csak az adott adatbiztonsági eseményre való reakció, hanem a hasonló események proaktív módon

[77] Ariz. Rev. Stat. § 44-7501 A.

[78] Me. Rev. Stat. tit. 10 §§ 1348

[79] **Bank sues Google for identity of Gmail user** http://www.theregister.co.uk/2009/09/23/google_sued_for_gmail_user_identity/

történő megelőzése.

### 1.3 Kivételek az értesítési kötelezettség alól

Az USA egyes tagállamainak jogszabályai szerint csak a „jelentős" (*material*) veszély váltja ki az értesítési kötelezettséget. Indiana államban[80] például az értesítési kötelezettség csak abban az esetben kötelező, ha az adatbiztonsági esemény valamely indianai lakost érintő személyiséggel való megtévesztéshez (*identity deception*), személyiséglopáshoz vagy csaláshoz vezetne. Iowaban[81] a sérelemnek pénzügyi természetűnek kell lennie.

A vonatkozó floridai jogszabály alapján[82] nincs szükség az értesítésre, ha az ügy megfelelő kivizsgálása, vagy az illetékes hatósággal való konzultáció után az adatkezelő ésszerűen feltételezi, hogy az adatbiztonsági esemény nem okozott, és nem okozhat kárt azon személyeknek, akiknek a személyes adatait harmadik személyek megszerezték vagy azokhoz hozzáfértek. A vizsgálat eredményét írásban kell lefolytatni és öt évig meg kell őrizni. A vizsgálat lefolytatásának elmulasztása, vagy a dokumentum-megőrzési kötelezettség megszegése 50.000 USD bírságot von maga után. Alaszka vonatkozó jogszabálya a floridai jogszabályhoz hasonló kivételt tartalmaz, és azt is megállapítja, hogy a dokumentáció nem minősül a nyilvánosság számára hozzáférhető közérdekű adatnak.[83]

Az USA számos tagállamában, például Arizonában, az értesítési kötelezettség teljesítésének előfeltétele, hogy az adatbiztonsági esemény az érintett személynek jelentős gazdasági kart okozzon, vagy feltételezhetően ilyen kárt okozhasson. A fentiek mellett az érintett személy nem köteles az adott rendszert érintő adatbiztonsági eseményről értesítést küldeni, amennyiben az illetékes hatóság ésszerű vizsgálatot követően megállapítja, hogy a rendszerrel kapcsolatos adatbiztonsági esemény nem valósult meg, és ésszerűen nem a várható, hogy megvalósuljon.[84] Washington állam vonatkozó jogszabálya szerint a biztonsági rendszer technikai sérelmét nem köteles az érintett magánszemély vagy társaság felfedni, ha ésszerűen nem várható, hogy ennek következtében az érintett ügyfelek bűncselekmény áldozataivá válnak.[85]

Az adatbiztonsági esemény által érintett személyes adatra nem minden esetben vonatkozik az értesítési kötelezettség: egy titkosított adat ugyanis harmadik személyek számára használhatatlan lehet, így az ilyen adatok kiemelt védelmére sincs feltétlenül szükség. Néhány szabályozás szerint

80 Ind. Code §§ 24-4.9-3-1
81 Iowa Code § 715C.1 (2008 S.F. 2308
82 Fla. Stat. § 817.5681 (10)
83 Alaska Stat. § 45.48.010 (c)
84 Ariz. Rev. Stat. § 44-7501 G.
85 Wash. Rev. Code § 19.255.010 (10) (d)

azonban, mint például Indiana államban[86], az értesítési kötelezettség a titkosított személyes adatra is kiterjed, de csak abban az esetben, ha az adatot megszerző harmadik fél hozzáfért, vagy hozzáférhet a titkosítási kulcshoz. Arizona állam[87] és Iowa állam[88] jogszabályai a „titkosított személyes adat" fogalmát is részletesen meghatározzák: eszerint a „titkosítás" jelentése például olyan eljárás használata, amellyel az adatokat olyan formába lehet átalakítani, hogy a titkos eljárás vagy kulcs nélkül olvashatatlanok vagy használhatatlanok. New Hampshire állam jogszabálya alapján titkosítás esetén már az adatok értelmezhetőségének „kis valószínűsége" esetén is köteles az adatkezelő értesítési kötelezettségét teljesíteni. A jogszabály azt is tisztázza, hogy az adatok nem tekinthetők titkosítottak, ha továbbításukra a hozzáférésükhöz szükséges kulccsal, biztonsági kóddal, hozzáférési kóddal vagy jelszóval együtt került sor.[89] Arizona állam jogszabálya szerint[90] az értesítési kötelezettség által érintett adatnak "nem titkosítottak" vagy nem „megfejthetőnek" kell lenniük. A „megfejthetőség" jelentése az adat oly módon történő megváltoztatása vagy összekapcsolása, hogy az adatgazda társadalombiztosítási számának, jogosítványa számának, személyazonosító számának, bankszámlaszámának, bankkártya számának legfeljebb utolsó négy számjegye a személyes adat részeként hozzáférhetővé válik.

*Az e-Privacy Irányelv rendelkezései:*

Az e-Privacy Irányelv értelmében nem kell az érintett előfizetőt vagy magánszemélyt értesíteni a személyes adataival való visszaélésről, ha a szolgáltatásnyújtó a hatáskörrel rendelkező hatóságnak kielégítően igazolni tudja, hogy végrehajtotta a megfelelő technikai védelmi intézkedéseket, illetve, hogy ezen intézkedéseket alkalmazták a biztonság sérelmével érintett adatok tekintetében. Az ilyen technológiai védelmi intézkedéseknek értelmezhetetlenné kell tenniük az adatokat az azokhoz való hozzáféréshez engedéllyel nem rendelkező személyek számára. Az érintett előfizetők vagy magánszemélyek értesítésére irányuló szolgáltatói kötelezettség sérelme nélkül, ha a szolgáltató még nem értesítette az előfizetőt vagy magánszemélyt a személyes adatok megsértéséről, az illetékes nemzeti hatóság kötelezheti erre, miután megfontolta a biztonság megsértésének várható hátrányos hatásait.[91]

---

86 Ind. Code §§ 24-4.9-3-1

87 Ariz. Rev. Stat. § 44-7501 L. 3.

88 Iowa Code § 715C.1 (2008 S.F. 2308)

89 N.H. Rev. Stat. §§ 359-C:19

90 Ariz. Rev. Stat. § 44-7501 L. 1.

91 e-Privacy Irányelv 4. cikk (3)

*Megfontolásra érdemes kérdések az e-Privacy Irányelv implementációja során:*

- Az értesítési kötelezettség alóli kivételeket az egyes tagállami szabályozásokban is arra figyelemmel kell meghatározni, hogy mikor kerülhetnek az adatok, illetve az érintett személyek tényleges és komoly veszélybe. Ez különösen nehéz lehet, mert a "személyes adatok", az e-Privacy Irányelv pedig az „adatbiztonsági esemény" fogalmát az EU Adatvédelmi Irányelve és az e-Privacy Irányelv nagyon tágan definiálja. Az adatbiztonsági értesítés azonban nem lehet szükségtelenül gyakori és nem vonhat el ésszerűtlen mennyiségű erőforrást sem az adatkezelőtől, sem az adatvédelmi hatóságtól. Az értesítési kötelezettségek alól való kivételek meghatározása során is figyelembe kell venni, hogy a jelentős kockázatok hiányában, szinte „automatikusan" küldött adatbiztonsági értesítéseket az érintett adatgazdák nem veszik majd komolyan, vagy zavarónak, ijesztőnek tartják, és ez problémát okozhat, ha a veszély valóban komoly. Fontos lenne meghatározni, hogy a csak néhány személyt érintő, vagy jelentős kockázatot nem hordozó adatbiztonsági eseményről nem feltétlenül szükséges értesíteni az illetékes hatóságokat, mert a relatíve kis jelentőségű eseményekről való túl sok értesítést a hatóságok rendelkezésre álló erőforrásokkal nem lehet kezelni. A tagállami szabályozások megalkotásakor fontos tehát figyelni arra, hogy az értesítési kötelezettség hatálya csak a valóban fontos eseményekre terjedjen ki. Az amerikai példák alapján ilyen lehet például, ha különleges adatok érintettek, kiskorúak érintettek, bűncselekmény veszélye áll fenn, ismétlődő eseményről van szó, jelentős számú adatgazda érintett vagy anyagi kár merülhet fel. Egyes adatkezelők – pl. egészségügyi adatok kezelőire vagy hitelintézetekre – természetesen kivonhatók a kivételek alól, az általuk kezelt speciális adatkörre tekintettel.
- Tekintettel arra, hogy a technikai védelmi intézkedések megfelelőségét az egyes hatáskörrel rendelkező hatóságok tagállamonként vizsgálják, az egyes országok szabályai ezáltal várhatóan eltérőek lesznek. Egy-egy adatbiztonsági esemény viszont akár több országot is érinthet, így fontos, hogy az egyes hatóságok egységes – akár európai szinten meghatározott – szempontokat és határidőket alkalmazzanak a megfelelőség értékelésére.
- Felmerül továbbá az a gyakorlati kérdés, hogy mi alapján tudja az adatkezelő megalapozottan eldönteni, mi történhet az ellenőrzése alól kikerült adatokkal, és

ennek megfelelően dönteni az értesítési kötelezettség teljesítéséről, vagy nem teljesítéséről? Hasznos lenne az adatkezelőknek, ha az illetékes hatóságok részletes iránymutatásokat bocsátanának ki ezzel kapcsolatban.

- Érdemes kiemelni, hogy Magyarországon az érintett személyek közvetlen értesítésének elrendelésére a Nemzeti Hírközlési és Média Hatóság (NMHH) az Adatvédelmi Biztos véleményének kikérését követően jogosult.[92] Gyakorlati szempontból egy újabb állami szereplő – jelen esetben az Adatvédelmi Biztos - bevonása a bejelentési kötelezettséggel kapcsolatos folyamatba nem tűnik túl hatékonynak: tekintettel arra, hogy egy adatbiztonsági eseményre való reakció gyors és effektív ügyintézését igényel, az újabb szereplő bevonása szükségtelenül lelassítaná a folyamatot, nem beszélve ennek emberi erőforrás- és költségvonzatáról: mind az NMHH-nak, mind az Adatvédelmi Biztosnak külön személyzetet kell fenntartania erre az esetre. Véleményünk szerin mindegy, hogy a jogszabály alapján az NMHH vagy az Adatvédelmi Biztos intézkedik az adatbiztonsági eseményekkel kapcsolatban, a lényeg, hogy az eljáró hatósági személyzetnek megfelelő felkészültséggel kell rendelkezniük ahhoz, hogy önállóan, társhatóság bevonása nélkül képesek legyenek eljárni az esettel kapcsolatban.
- Az e-Privacy Irányelv nem tartalmaz az amerikai szabályozáshoz hasonló kifejezett utalást az adatok titkosításának vizsgálatára az adatbiztonsági esemény elbírálása során. Hasznos lenne, ha az adatbiztonsági értesítési eljárások során alkalmazandó hatósági iránymutatások pontosan kitérnének a lehetséges megoldásokra, tekintettel arra, hogy az adatok titkosítása az adatkezelők gyakorlatában egyre inkább elterjedt.

### 1.4 Harmadik személyek által kezelt / feldolgozott adatokkal kapcsolatos értesítési kötelezettség

A harmadik személyek által kezelt / feldolgozott adatokkal összefüggő adatbiztonsági eseménnyel kapcsolatos értesítési kötelezettséget a legtöbb USA tagállam jogszabálya szintén hasonlóan kezeli.

Bármely, elektronikus formában harmadik személy tulajdonában levő személyes adatot kezelő személy köteles az adatgazdát vagy az adatkezeléshez hozzájáruló személyt értesíteni az adatbiztonsági esemény felfedezését követően haladéktalanul értesíteni, ha a személyes adathoz harmadik személyek hozzáfértek, vagy hozzáférhettek.[93]

[92] Eht. 156. § (6)

[93] Cal. Civ. Code 1798.82. (b)

Az adatkezelő felhatalmazása alapján adatfeldolgozását végző személy és az adatkezelő külön megállapodásban rendezhetik, hogy az értesítési kötelezettséget melyikük teljesíti. Ha ezzel kapcsolatban a két fél nem tud megállapodni, az érintett adatgazdával közvetlen szerződéses viszonyban álló fél (adatkezelő) köteles az értesítési kötelezettséget teljesíteni. A legtöbb tagállam (pl. Washington[94], Alaszka[95], Arizona[96], Delaware[97], New York[98]) jogszabálya a fentiekben hasonló rendelkezéseket tartalmaz. Néhány állam azonnali értesítési kötelezettséget, néhány állam pedig meghatározott határidőt (általában 10 napot) ír elő erre.

Alaszka állam jogszabálya kifejezett együttműködési kötelezettséget ír elő az érintett személyek számára, vagyis az adatbiztonsági eseményre vonatkozó információk rendelkezésére bocsátását, az üzleti titoknak minősülő információk kivételével.

*Megfontolásra érdemes kérdések az e-Privacy Irányelv implementációja során:*

- Ha az e-Privacy Irányelv nyomán az egyes EU tagállamokban is elfogadásra kerülnek az adatbiztonsági értesítéssel kapcsolatos részletes jogszabályok, hasonló különbségtétel szükséges a „saját adatok" és a „harmadik személyek által kezelt / feldolgozott" adatok között. Ennek oka, hogy az Adatvédelmi Irányelv az adatkezelőket és az adatfeldolgozókat szintén külön kezeli - mint ismeretes, ez a magyar szabályozásban nem igazán sikeresen került átvételre, sajnos az új adatvédelmi törvényben sem.
- Fontos lehet továbbá, hogy az adatbiztonsági értesítési eljárások során alkalmazandó hatósági iránymutatások részletesen meghatározzák az adatkezelők és az adatfeldolgozók együttműködésének módját (pl. határidők, felelősségi kör, kommunikációs folyamat) az adatbiztonsági esemény kezelése során – akár minta-szerződéses rendelkezések kibocsátása formájában is.

## 2. A kötelezettek köre

A kötelezettek köre az USA-ban tagállamonként változik. Egyes adatbiztonsági értesítési jogszabályok

94 Wash. Rev. Code § 19.255.010 (2)
95 Alaska Stat. § 45.48.070
96 Ariz. Rev. Stat. § 44-7501 B.
97 Del. Code tit. 6, § 12B-102 et seq.
98 N.Y. Gen. Bus. Law § 899-aa

személyi hatálya nem terjed ki természetes személy vagy kormányzati szerv adatkezelőkre. Mindazonáltal a „személy" fogalma általában elég széles kört foglal magában: magánszemélyek, cégek, alapítványok, valamint maga az állam, illetve kormányszervek is. Egyes államokban az állami és a magánszektorra különböző értesítési kötelezettségek irányadók.

Az adatkezelő szervezetének mérete is fontos lehet. Alaszkában[99] például, a (kötelezett) „személy" jelentése: gazdálkodó személy, kormányszerv, vagy 10 munkavállalónál többet foglalkoztató munkáltató.

Georgia állam vonatkozó jogszabálya is érdekes lehet, mert úgy tűnik, hogy csak a „hivatásos" adatkezelőkre irányadó: az adatbiztonsági értesítési kötelezettségek kizárólag arra a személyre vagy entitásra vonatkoznak, amely ellenérték fejében részben vagy egészben személyes adatok üzletszerű gyűjtésével, összeállításával, értékelésével, összekapcsolásával, továbbításával foglalkozik, elsősorban abból a célból, hogy független harmadik személyek számára az érintett személyes adatokkal kapcsolatban információt nyújtson. (Nem tartoznak ide ugyanakkor az elsődlegesen közlekedésbiztonsági, bűnüldözési vagy engedélyezési célból személyes adatokat gyűjtő állami szervek.)[100]

*Az EU Adatvédelmi Irányelve és az e-Privacy Irányelv rendelkezései:*

Az EU Adatvédelmi Irányelve és az e-Privacy Irányelv nem tesz kivételt: az általuk meghatározott kötelezettségek függetlenek az adatkezelő szervezetének nagyságától. Az adatgazdák számára ez a megközelítés szimpatikusabb lehet – a vonatkozó adatvédelmi kötelezettségeknek való megfelelés nem függhet a társaság tulajdonosi szerkezetétől vagy szervezetének méretétől, és az általános adatbiztonsági értesítési kötelezettségek nem jelentenek olyan ésszerűtlen többletterhet, ami indokolná a kisebb adatkezelők mentesítését a kötelezettségek alól. A tendencia egyébként is az, hogy sajnos a hackerbetörések egyre inkább érintik a kisebb cégeket is, mert ezeknek a vállalkozásoknak kevesebb anyagi erőforrás és technikai know-how áll rendelkezésre az adatbiztonsági események megelőzésére.[101]

*Megfontolásra érdemes kérdés az e-Privacy Irányelv implementációja során:*

---

[99] Alaska Stat. § 45.48.090 (2)

[100] Ga. Code §§ 10-1-911

[101] **Hackers Shift Attacks to Small Firms**
http://online.wsj.com/article/SB10001424052702304567604576454173706460768.html

- Az EU-s szabályozásban gyakorlati szempontból hasznos lehet az egy cégcsoporton belüli társaságok egy adatkezelőként való meghatározása, akárcsak legalább az adatbiztonsági értesítési kötelezettségek teljesítése tekintetében. Előfordulhat ugyanis, hogy az adatbiztonsági esemény több országot is érint – egy adatkezelő ebben az esetben könnyebben és hatékonyabban koordinálhatja az eseményre adott választ, és ez végső soron az adatgazdák érdekét szolgálja. Az EU Adatvédelmi Irányelve és az e-Privacy Irányelv sajnos egyelőre nem ennyire rugalmas, és ez nem könnyíti meg a többszintű vállalati struktúrában működő nemzetközi vállalatok napi szintű működését (pl. adattovábbítás egy egységes, világszintű HR adatbázisba), sőt, gyakran ésszerűtlen anyagi költségeket és emberi erőforrások igénybevételét okoz az érintett adatkezelők oldalán. A szabályozás egyszerűsítésével rengeteg adminisztrációtól lehetne megmenteni a cégeket, ugyanakkor az adatgazdákat sem fenyegeti veszély, mert ma már a gyakorlatban megszokottak a cégcsoportokon belüli külföldi adattárolások, adattovábbítások, és egy jó piaci hírnévvel rendelkező adatkezelő üzleti szempontból sem engedheti meg magának, hogy elmulassza a technikailag legmegfelelőbb adatbiztonsági intézkedések megtételét és az értesítési kötelezettségek teljesítését.

### 3. A „személyes adatok” meghatározása

Az USA-ban majdnem minden tagállam jogszabálya tartalmaz példákat, vagy kifejezett felsorolást a személyes adatok tekintetében.

Florida állam vonatkozó jogszabálya[102] szerint például „személyes adat” az érintett személy keresztneve, keresztnevének kezdőbetűje és vezetékneve, második keresztneve és vezetékneve, a következő nem titkosított adatok bármelyikével együttesen:

- társadalombiztosítási azonosító;
- jogosítvány száma vagy személyi igazolvány szám;
- bankszámlaszám, hitelkártyaszám, az érintett bankszámlájához való hozzáféréshez szükséges biztonsági kóddal, belépési kóddal vagy jelszóval együtt.

[102] Fla. Stat. § 817.5681 (5)

A többi állam – pl. Alaszka[103], Arizona[104], Delaware[105], New York[106], Washington[107], Illinois[108] - vonatkozó jogszabályai nagyjából hasonló meghatározást tartalmaznak. Egyes adatvédelmi kötelezettségek tekintetében a kaliforniai jogszabály további feltételeket tartalmaz[109]: a személyes adatot olyan adatként határozza meg, amely egy bizonyos személyt azonosít, hozzá kapcsolódik, leír, vagy ezekre alkalmas, ideértve például a nevét, aláírását, társadalombiztosítási számát, fizikai vonásait vagy személyleírását, címét, telefonszámát, útlevélszámát, jogosítvány számát, személyazonosító igazolvány számát, biztosítási kötvény számát, tanulmányait, munkahelyeit, bankszámlaszámát, hitelkártyaszámát, egyéb pénzügyi információit, egészségügyi adatait, egészségbiztosítási adatait.

Gyakorlati szempontokra figyelemmel Észak- Dakota állam jogszabálya[110] a következő adatokat is személyes adatként határozza meg (ha az adott személy nevével együttesen kerülnek felhasználásra): az adott személy munkáltatója által az adott személyhez rendelt azonosítót, az illető elektronikus vagy egyéb digitális aláírását, az illető születési idejét, anyja leánykori nevét.

Iowa állam vonatkozó jogszabálya [111] a legutóbbi technológiai fejlesztéseket is figyelembe veszi és az „egyedi elektronikus azonosítót vagy *routing code*-ot" (az illető bankszámlájához való hozzáféréshez szükséges biztonsági kóddal, belépési kóddal vagy jelszóval együttesen felhasználva) és egyedi biometrikus adatokat (úgymint ujjlenyomat, retina vagy íriszkép, vagy egyéb egyéni fizikai azonosító, vagy biometrikus adat digitális megjelenítése) is személyes adatként határoz meg.

Észak-Karolina állam jogszabálya szerint például elektronikus azonosítók, elektronikus postacímek, internetes számlaszámok, internetes azonosítószámok, szülők házasság előtti neve, és a jelszavak nem minősülnek személyes adatnak, kivéve, ha felhasználásukkal hozzá lehet férni az adott személy bankszámlához vagy pénzeszközeihez.[112]

A nyilvánosság számára jogszerű úton (pl. nyilvántartásokból) hozzáférhető információk értelemszerűen – és ezt a legtöbb jogszabály is kimondja – általában nem tartoznak az értesítési kötelezettség hatálya alá. Számos tagállamban a „személyes adat" fogalma nem vonatkozik a „média által széles körben" (*widely distributed by the media*) terjesztett információra. Ohio állam jogszabálya szerint[113], például nem minősül „személyes adatnak" a nyilvánosság számára valamely szövetségi, állami, vagy helyi szintű nyilvántartásból jogszerűen hozzáférhető információ vagy valamely, a média által széles körben

103 Alaska Stat. § 45.48.090 (7)
104 Ariz. Rev. Stat. § 44-7501 L. 6.
105 Del. Code tit. 6, § 12B-101 (4)
106 N.Y. Gen. Bus. Law § 899-aa 5.
107 Wash. Rev. Code § 19.255.010 (5)-(6)
108 815 ILCS 530/5 Sec. 5.
109 1798.80. (d) ( Cal. Civ. Code)
110 N.D. Cent. Code § 51-30-01
111 Iowa Code § 715C.1 (2008 S.F. 2308)
112 N.C. Gen. Stat § 75-65
113 Ohio Rev. Code §§ 1347.12 (A) (6) (b) és Ohio Rev. Code §§ 1349.19 (A) (7) (b)

terjesztett információ, a következők szerint:

- valamely újságban folyóiratban, magazinban, vagy rádiós, illetve televízióadásban jóhiszeműen megjelent hír, szerkesztői közlemény, reklám;
- valamely riporter, tudósító, hírügynökség által a fenti médiumok számára jóhiszeműen összegyűjtött, illetve átadott információ vagy hír;
- valamely egyesülés vagy szervezet számára jóhiszeműen készített vagy átadott publikáció.

*Megfontolásra érdemes kérdések az e-Privacy Irányelv implementációja során:*

- Az EU Adatvédelmi Irányelve nem tartalmazza a személyes adatok részletes meghatározását. A „személyes adatok" meghatározása általános szinten történik, és csak az egyes adatvédelmi hatóságok iránymutatása segíthet eldönteni, hogy egy bizonyos információ személyes adatnak minősül-e. Ezzel szemben az USA-ban majdnem minden tagállam jogszabálya tartalmaz példákat, vagy kifejezett felsorolást a személyes adatok tekintetében. Ez a megközelítés több segítséget nyújthat az adatkezelők számára – a személyes adatokat kezelő nem-jogász munkatársaik ugyanis nem biztos, hogy esetről-esetre értelmezni tudják az adatvédelmi jogszabályok általános meghatározásait. A jogszabályokkal és gyakorlati alkalmazásukkal kapcsolatos részletes oktatás hiányában így nem tudják megállapítani azt sem, hogy valamely információ a jogszabály által védett személyes adatnak minősül-e.
- Az EU Adatvédelmi Irányelve nem tartalmaz az USA szabályozásához hasonló kivételt a „széles körben terjesztett" személyes adatok tekintetében. Az EU-ban egy hasonló megközelítés az egyes országok kulturális sajátosságaitól és gyakorlatától függhet. Mindazonáltal a „széles körben terjesztett" személyes adatoknak az általánostól eltérő kezelése az egyes európai tagállamok jogalkotói számára megfontolandó lehet (különös tekintettel egyes személyes adatok széles körű hozzáférhetőségére, pl. a médiában vagy közösségi oldalakon). A kérdés már csak azért is érdekes, mert 2010 júliusában[114] a Skull Security biztonságtechnikai cég egyik munkatársa a nyilvánosan hozzáférhető

[114] **Facebook Hacking, Security, and Privacy Concerns** https://www.infosecisland.com/blogview/9361-Facebook-Hacking-Security-and-Privacy-Concerns.html **Százmillió Facebook-felhasználó adatai kerültek ki a netre** http://index.hu/tech/net/2010/07/29/100_millio_facebook-felhasznalo_adatai_kerultek_ki_a_netre/

Facebook profilokból (és a kapcsolódó személyes adatokból) állított össze adatbázist tett hozzáférhetővé az interneten, rávilágítva ezzel, hogy a felhasználók milyen könnyelműen osztják meg személyes adataikat a nyilvánossággal. Magyarországon nem kell megtéríteni a kárt a személyes adatok jogellenes kezelésével kapcsolatban, ha az a károsult súlyosan gondatlan magatartásából származott - az Adatvédelmi Biztos is kiemelte többek között az új adatvédelmi törvény előzetes észrevételezése során, hogy ez esetleg a közösségi oldalakon adataikat meggondolatlanul nyilvánosságra hozó felhasználóira is vonatkoztatható.[115] Álláspontunk szerint is indokolt lehet, hogy az adatkezelőnek lehetősége legyen mentesülnie felelőssége alól, ha az adatgazda maga hozta nyilvánosságra korábban azt az adatot, amivel kapcsolatban később visszaélés történt. Az internethasználat, különösen a közösségi oldalak elterjedtségére tekintettel ma már a felhasználóktól is elvárható lehet egy bizonyos minimális adatbiztonsági és adatvédelmi ismeret, különös tekintettel arra, hogy ne hozzák nyilvánosságra, ne osszák meg indokolatlanul személyes adataikat – ha mégis így döntenek, akkor viszont csak indokolt esetben háríthassák a felelősséget harmadik személyre.

## 4. Az „adatbiztonsági esemény” meghatározása

Az USA-ban az „adatbiztonsági esemény” meghatározása meghatározását a legtöbb jogszabály megpróbálja a lehető legspecifikusabban definiálni.

Az „adatbiztonsági esemény” fogalmát a kaliforniai jogszabály például a következőképpen határozza meg: számítógépes adat jogtalan megszerzése, amely veszélyezteti az adott magánszemély vagy vállalkozás által kezelt információk biztonságát, bizalmas természetét, vagy integritását. Valamely személyes adatnak az adatkezelő egy munkavállalója vagy megbízottja általi kizárólag az adatkezelő belső céljára való jóhiszemű megszerzése nem minősül adatbiztonsági eseménynek, ha a személyes adat nem kerül jogtalanul felhasználásra vagy továbbításra.[116]

Az egyes tagállamok – pl. Alaszka[117] and Delaware[118] – vonatkozó jogszabályainak többsége hasonló definíciót tartalmaz. Alaszkában[119], az adatkezelő által kezelt személyes adat biztonságát, bizalmas természetét vagy integritását veszélyeztető jogtalan hozzáférésnek “ésszerű valószínűsége” szintén

115 Ügyszám: ABI-1788-2/2011/Jhttp://abiweb.obh.hu/abi/index.php?menu=aktualis/allasfoglalasok/2011&dok=1788_J_2011-2

116 1798.82. (d) (Cal. Civ. Code)

117 Alaska Stat. § 45.48.050

118 Del. Code tit. 6, § 12B-101 et seq. (1)

119 Alaska Stat. § 45.48.090 (1)

"adatbiztonsági eseménynek" minősül. A "hozzáférés" magában foglalja az információnak (i) fénymásolás, faxüzenet vagy más papíralapú úton; (ii) az információ numerikus formában való beolvasására, írására vagy tárolására alkalmas eszköz által (pl. számítógép); vagy (iii) a fentiektől eltérő módszer által való megszerzését.

New York állam vonatkozó jogszabálya[120] a definíciót a következők szerint finomítja:

*„Annak megállapítása érdekében, hogy az információt illetéktelen vagy megfelelő felhatalmazással nem rendelkező személyek megszerezték, vagy ésszerű valószínűséggel megszerezhették, az érintett adatkezelőnek a következő szempontokat kell figyelembe vennie:*

- *annak jelét, hogy az információ az illetéktelen személynek (fizikailag) a birtokában és ellenőrzése alatt van, pl. számítógép vagy egyéb adathordozó ellopása vagy elvesztése; vagy*
- *annak jelét, hogy az információt letöltötték vagy átmásolták; vagy*
- *annak jelét, hogy az információt illetéktelen személy felhasználta, pl. bankszámla hamis személyazonossággal való megnyitása vagy egyéb „személyiséglopás" (identity theft)*".

Ohio vonatkozó jogszabálya az adatbiztonsági esemény által érintett „rendszert" is külön meghatározza. Jelentése: „*bármely rendszerszerűen működtetett, összegyűjtött vagy csoportosított adatnyilvántartás, amelyből az érintett személy neve, vagy azonosítószáma, jele, egyéb azonosítója alapján személyes adat és az információhoz nem jogosulatlanul fértek hozzá*". Nem minősül "rendszernek" a történelmi jellegű archívum vagy a nyilvánosan hozzáférhető nyilvántartás, amennyiben az információhoz való hozzáférés nem érintheti az érintett személyt hátrányosan.[121]

*Az e-Privacy Irányelv rendelkezései:*

A módosított e-Privacy Irányelvben meghatározásra került a „személyes adatok megsértése" fogalma a következők szerint: „*a biztonság olyan megsértése, amely a Közösségben nyilvánosan elérhető*

120 N.Y. Gen. Bus. Law § 899-aa (c)

121 Ohio Rev. Code §§ 1347.12 (A) (11) és Ohio Rev. Code §§ 1349.19 (A) (10)

*hírközlési szolgáltatások nyújtásával összefüggésben továbbított, tárolt vagy más módon feldolgozott személyes adatok véletlen vagy jogellenes megsemmisítését, elveszítését, módosítását, jogosulatlan felfedését vagy az azokhoz való jogosulatlan hozzáférést eredményezi".*[122]

*Megfontolásra érdemes kérdés az e-Privacy Irányelv implementációja során:*

- Fontos, hogy a csak általánosságban definiált „adatbiztonsági esemény" fogalma az egyes tagállamokban egységesen kerüljön értelmezésre, és az illetékes adatvédelmi hatóságok lehetőség szerint konkrét példák felsorolásával tájékoztassák az adatkezelőket, hogy pontosan mely események is esnek az értesítési kötelezettség alá. Az adatkezelők nem-jogász munkatársainak ugyanis egy lehetséges adatbiztonsági esemény esetén a lehetséges veszélyek sürgős elhárítása közben nem feltétlenül vannak megfelelő erőforrásaik és idejük a túl széles körűen megfogalmazott jogszabályi definíciók értelmezésére. Az „adatbiztonsági esemény" meghatározása tartalmazhatná például az adatvesztés érzékenységének értékeléséhez küszöbszámokat és a kikerült adathoz való hozzáférhetőség lehetséges eseteit.

## 5. Az értesítés késleltetése

Az értesítés az USA majdnem minden tagállamának jogszabálya alapján késleltethető bűnüldözési célból, ha a bűnüldöző szerv véleménye szerint az értesítés gátolná a nyomozást. Az értesítési kötelezettség teljesítésére nyitva álló idő azt követően kezdődik, hogy az adatkezelő értesítést kap arról, hogy az értesítés nem veszélyezteti a nyomozást. Ilyen kivételt tartalmaz például Alaszka[123], Arizona[124] Washington[125], New York[126] és Kalifornia[127] jogszabálya. A vonatkozó Hawaii-i jogszabály szerint az értesítést írásban kell megtenni, illetve az illetékes hatóságnak a részleteket (pl. az értesítés visszatartását kérő tisztségviselő és az érintett nyomozó nevét) egyértelműen, írásban dokumentálnia kell.[128] Ohio államban az értesítést abban az esetben is késleltetni lehet, ha az illetékes hatóság megállapítja, hogy az értesítés nem csak a nyomozást hátráltatná, de a nemzetbiztonságot is

122 e-Privacy Irányelv 2. cikk (h)
123 Alaska Stat. § 45.48.020
124 Ariz. Rev. Stat. § 44-7501 C.
125 Wash. Rev. Code § 19.255.010 (3)
126 N.Y. Gen. Bus. Law § 899-aa
127 1798.82. (c) (Cal. Civ. Code)
128 Haw. Rev. Stat. § 487N-2 (c)

veszélyeztetné.[129]

*Az e-Privacy Irányelv rendelkezései:*

A Módosító Irányelv preambuluma[130] előírja, hogy a „*szabályoknak és eljárásoknak figyelembe kell venniük továbbá a bűnüldöző hatóságok jogos érdekeit olyan esetekben, amikor az idő előtti feltárás szükségtelenül veszélyeztethetné a jogsértés körülményeinek kivizsgálását*".

*Megfontolásra érdemes kérdés az e-Privacy Irányelv implementációja során:*

- Az európai infokommunikációs iparágban az érintett adatkezelők és az egyes illetékes hatóságok együttműködése különösen fontos, így az elfogadásra kerülő, az adatbiztonsági értesítéseket szabályozó tagállami szabályozásoknak ezeket a helyzeteket is kezelniük kell. Fontos az irányadó emberi jogokat tiszteletben tartani, a hírhedt adatmegőrzési irányelvhez hasonló alkotmányossági aggályok elkerülése végett. Tekintettel arra, hogy az állami szervek ügymenete a magánszektorhoz képest lassabb, az értesítési kötelezettségek és az együttműködés során fontos specifikus határidőket és feladatköröket szabni az egyes felek részére. A határidők meghatározása során különösen figyelni kell arra, hogy az adatbiztonsági értesítés elküldésének indokolatlan késedelme jelentős károkat okozhat mind az adatkezelő, mind az adatgazdák számára.

## 6. Egyéb címzettek értesítése

Az USA-ban az adatbiztonsági esemény jellegétől függően előfordulhat, hogy egyes hatóságokat is értesíteni kell - általában az érintett személyek számától függően, de vannak általános jellegű kötelezettségek is.

Alaszkában például[131], ha az adatkezelő a tagállam több mint 1.000 lakosát lenne köteles értesíteni, az adatkezelőnek az országos szinten fogyasztói adatokat összeállító és tároló hitelinformációs szervezetet (*credit reporting agency*) is tájékoztatnia kell az adott tagállam lakosainak küldendő értesítés időzítéséről, kézbesítési módjáról és tartalmáról. Az adatkezelő ugyanakkor nem köteles a

[129] Ohio Rev. Code §§ 1347.12 (D)
[130] Módosító Irányelv (64) preambulum-bekezdése
[131] Alaska Stat. § 45.48.040

hitelinformációs szervezet számára az érintett személyek nevét vagy más személyes adatát átadni. Hawaii jogszabálya szerint az illetékes fogyasztóvédelmi hatóságot is értesíteni kell.[132] Az érintett személyek száma tagállamonként változik: New York-ban például az egyéb címzetteket 5.000 érintett személy esetén kell értesíteni.

Illinois-ban[133] az (elektronikus rendszert vagy fizikai dokumentumokat érintő) adatbiztonsági esemény által érintett állami adatkezelők az esemény észlelését követő öt munkanapon belül kötelesek az eseményt jelenteni az illetékes szerv (*General Assembly*) részére, az esemény(ek) ismertetésével és a helyzet orvoslásával és a hasonló (elektronikus rendszert vagy fizikai dokumentumokat érintő) helyzetek jövőbeli megelőzésével kapcsolatban megtett intézkedések felsorolásával. A fentiek szerint jelentést tevő állami szervek éves jelentést is kötelesek készíteni, az őket érintő összes (elektronikus rendszert vagy fizikai dokumentumokat érintő) adatbiztonsági esemény és a hasonló helyzetek jövőbeli megelőzésével kapcsolatban megtett intézkedések felsorolásával.

New York állam jogszabálya szerint[134] ha New York állam valamely lakosának adatbiztonsági értesítést kell küldeni, az adatkezelő személy vagy cég az államügyészt (*state attorney general*), valamint az érintett fogyasztóvédelmi szervezetet (*consumer protection board*) és az állam cyber-biztonsági és kritikus infrastruktúrát koordináló hivatalát is köteles értesíteni az értesítések megtételének időpontjáról, az értesítések tartalmáról és elküldésük módjától, továbbá az érintett személyek hozzávetőleges számáról.

Egyes jogszabályok felhatalmazzák az illetékes hatóságokat az adatbiztonsági esemény természetének meghatározására és a megfelelő (hatósági) intézkedések megtételére a problémák megoldása érdekében, saját hatáskörben, vagy az adatkezelővel, illetve adatfeldolgozóval való együttműködésben.

*Megfontolásra érdemes kérdés az e-Privacy Irányelv implementációja során:*

- Európában az illetékes infokommunikációs vagy adatvédelmi hatóságok megfelelő címzettjei az adatbiztonsági értesítéseknek. Fontos azonban, hogy valóban a legmegfelelőbb hatóságot terhelje ez a feladat – az illetékes személyzet felkészítése az adatbiztonsági eseményekre ugyanis jelentős időt és ráfordítást igényel, így később nem biztos, hogy lehetséges az adott hatóság kijelölésén változtatni. Érdemes továbbá

132 Haw. Rev. Stat. § 487N-2 (f)
133 815 ILCS 530/5 Sec. 25
134 N.Y. Gen. Bus. Law § 899-aa 8.

elkerülni az eljáró hatóságok szükségtelen „megkettőzését” – ahogyan, amint azt fent már említetésre került, Magyarországon sem szükséges feltétlenül egyszerre két hatóság – az NMHH és az Adatvédelmi Biztos – bevonása az adatbiztonsági események intézésébe.[135]

## 7. Az értesítés tartalma

Az USA-ban számos tagállam részletes követelményeket határoz meg az értesítés tartalmával kapcsolatban. New York államban[136] például, függetlenül az értesítés formájától, az értesítésnek tartalmaznia kell az értesítést küldő személy vagy cég elérhetőségének adatait, valamint a jogosulatlanul megszerzett (vagy vélhetően megszerzett) információk körét, ideértve a jogosulatlanul kikerült személyes adatoknak a megnevezését.

Az értesítésnek világosnak és érthetőnek kell lennie, és tartalmaznia kell a következőket:

- Az adatbiztonsági esemény általános leírása.
- A jogosulatlanul hozzáfért és megszerzett személyes adatok típusai.
- Az adatkezelő által a személyes adatokhoz való további jogosulatlan hozzáférés megakadályozása érdekében tett általános intézkedések.
- Egy telefonszám, amit az érintett személy további információért és segítségnyújtás kérése esetén hívhat.
- Figyelemfelhívás, hogy az érintett személy figyelje bankszámlakivonatait és ingyenes hitelinformációt (*credit report*).

Iowa[137] és Észak-Karolina[138] állam jogszabályai hasonló szabályokat tartalmaznak. Iowaban azonban az értesítésnek tartalmaznia kell az adatbiztonsági esemény hozzávetőleges időpontját, és a hitelinformációs szervezetek elérhetőségeit is. Nyugat-Virginia államban az adatkezelővel vagy adatfeldolgozóval való kapcsolatfelvételre használt telefonos elérhetőségnek vagy weboldalnak alkalmasnak kell lennie arra, hogy az érintett személy megismerje, a róla, vagy általánosságban más

135 Eht. 156. § (6)
136 N.Y. Gen. Bus. Law § 899-aa 7.
137 Iowa Code § 715C.1 (2008 S.F. 2308)
138 N.C. Gen. Stat § 75-65

személyekről tárolt személyes adatok körét, és azt is, hogy ténylegesen tároltak-e az adott személlyel kapcsolatosan adatokat.[139]

*Az e-Privacy Irányelv rendelkezései*

Az előfizetőnek vagy magánszemélynek szóló értesítés tartalmazza legalább a személyes adatok megsértésének jellegét és azokat az információs pontokat, ahol az előfizető további felvilágosítást kaphat, továbbá intézkedéseket javasol a személyes adatok megsértése lehetséges hátrányos hatásainak enyhítésére. Az illetékes nemzeti hatósághoz intézett értesítés ezen túlmenően leírja a személyes adatok megsértésének következményeit és az annak orvoslására a szolgáltató által javasolt vagy megtett intézkedéseket.[140] A magyarországi szabályozás rögzíti, hogy az NMHH iránymutatást adhat ki a bejelentési és értesítési kötelezettség teljesítésének a módjára, és a nyilvánosan elérhető elektronikus hírközlési szolgáltatók személyes adatok kezelésével kapcsolatos elérendő biztonsági szintre vonatkozó legjobb gyakorlatokról.[141]

*Megfontolásra érdemes kérdések az e-Privacy Irányelv implementációja során:*

- Világos szabályokat kellene meghatározni az értesítő levél formájára és tartalmára nézve (pl. az adatbiztonsági esemény jellegének egyértelmű meghatározása, az érintett magánszemély által teendő lépések stb.). Egyértelmű, hogy a szabályozó hatóságoknak ajánlásaikban mind az adatkezelők, mind az adatgazdák számára könnyen használható, ugyanakkor informatív értesítésmintákat szükséges kidolgozniuk. A legjobb megoldás az lenne, ha egy egységes, minden EU-s tagállamban használatos értesítési forma kerülne meghatározásra. A különböző értesítési minták használata a több tagállamban működő adatkezelőknek zavaró lehet, felesleges többletköltségeket, illetve adminisztratív feladatokat okozhat és ezáltal egy több országot érintő adatbiztonsági értesítés elküldése indokolatlan késedelmet szenvedhet, és jelentős károkat okozhat mind az adatkezelő, mind az adatgazdák számára. Ha az adatbiztonsági esemény több országot is érint, egy adatkezelő egy egységes értesítésminta használatával könnyebben és hatékonyabban koordinálhatja az

139 W.V. Code §§ 46A-2A-102 (d)
140 e-Privacy Irányelv 4. cikk (3)
141 Eht. 156. § (7)

eseményre adott válaszok összegyűjtését az érintett országokban, és ez végső soron az adatgazdák érdekét szolgálja.

- Kérdésként merül fel továbbá, hogy az értesítés tartalma csupán általános és informatív jellegű, vagy kötelezettséget is keletkeztet-e az adatkezelő oldalán egy-egy meghatározott intézkedés megtételére. Az ezzel kapcsolatos félreértések elkerülése érdekében nagyon fontos az értesítés megfelelő megfogalmazása, valamint az adatbiztonsági eseménnyel kapcsolatban tett minden intézkedés és kommunikáció megfelelő dokumentálása.
- Fontos arra figyelni, hogy az értesítési kötelezettség ne egy egyszerű adminisztratív és „reaktív" kötelezettség legyen, hanem proaktív módon ténylegesen az adott adatbiztonsági probléma megoldását szolgálja. Kezelni kell azt a helyzetet, ha az értesítés elküldését követően az ügyben újabb információk derülnek ki, és erről szükséges lehet értesíteni a hatóságokat, illetve az adatgazdákat. Elengedhetetlen továbbá az adatbiztonsági esemény következményeit is nyomon követni, és a fontosabb fejleményekről tájékoztatni az érintett feleket.
- Érdemes lehet az elektronikus hírközlési szektorban az előfizetőket már előzetesen értesíteni az adatbiztonsági értesítési kötelezettségek bevezetéséről, hogy „éles helyzetben" ne érje őket váratlanul egy ilyen értesítés. A nyilvánosságnak az új szabályokról való tájékoztatásában kulcsfontosságú szerepe van az illetékes hatóságoknak.

## 8. Az értesítés módja

Az USA legtöbb tagállamában, például Florida[142], Washington[143] és Kalifornia[144] államokban, az értesítést az alábbi módok valamelyikén lehet megtenni:

- Írásbeli értesítés;
- Elektronikus értesítés, ha az értesítésre köteles fél rendelkezik az érintett személy e-mail címével és az érintett személy hozzájárult az elektronikus úton való kommunikációhoz; vagy

[142] Fla. Stat. § 817.5681 (6)
[143] Wash. Rev. Code § 19.255.010 (7)
[144] 1798.82. (g) (Cal Civ. Code)

- Úgynevezett “helyettesítő értesítés”, ha az értesítésre köteles fél igazolja, hogy az értesítés költsége meghaladja a 250.000 USD-t, az értesítendő személyek köre meghaladja az 500.000-et, vagy nem állnak rendelkezésre megfelelő kapcsolattartási adatok.

A „helyettesítő értesítést” az alábbi formák mindegyikében kell megtenni:

- Elektronikus levél vagy e-mail (ha az értesítésre kötelezett fél rendelkezik az érintett személyek elektronikus elérhetőségével, illetve e-mail címével).
- Figyelemfelhívó értesítés az értesítésre kötelezett fél weboldalán (ha a kötelezett működtet weboldal-t).
- Értesítés egy nagyobb országos médium részére.

A „helyettesítő értesítések” feltételeként meghatározott költségek nagysága és az érintett személyek száma államonként változik.

Egyes jogszabályok, például Kalifornia vagy Delaware[145] államok jogszabályai szerint elektronikus úton értesítés csak a vonatkozó elektronikus aláírásról és elektronikus archiválásról szóló törvénynek megfelelően[146] tehető. Utah államban az írásbeli értesítést az érintett személy utolsó ismert postacímére kell küldeni.[147]

Ohio állam jogszabálya szerint[148], a weboldalon való közzététel mellett a „helyettesítő értesítést” egy helyi, az adatkezelő személy székhelye szerinti helységében terjesztett újságban, fizetett hirdetés formájában is meg kell tenni. A hirdetésnek megfelelő méretűnek (legalább negyed oldalasnak) kell lennie és három egymást követő héten legalább hetente egyszer közzé kell tenni.

New York állam vonatkozó jogszabálya[149] szintén hasonló értesítési módokat követel meg, elektronikus úton történő értesítés azonban csak akkor küldhető, ha az érintett személy kifejezetten hozzájárult az elektronikus kommunikációhoz és az adatkezelő köteles az egyes értesítéseteket egyenként nyilvántartani (naplózni). A hozzájárulás nem lehet feltétele az adatkezelővel való üzleti kapcsolatnak. A vonatkozó jogszabály a telefonos értesítést is lehetővé teszi, feltéve, ha az adatkezelő az ily módon

145 Del. Code tit. 6, § 12B-101 et seq. (3) c.
146 15 U.S.C. s. 7001 - Electronic Signatures in Global and National Commerce Act
147 Utah Code §§ 13-44-202
148 Ohio Rev. Code §§ 1347.12 (E) (5) és Ohio Rev. Code §§ 1349.19 (E) (5)
149 N.Y. Gen. Bus. Law § 899-aa 5.

tett értesítéseket egyenként nyilvántartja (naplózza). Arizona állam jogszabálya[150] nyilvántartási (naplózási) kötelezettség nélkül is lehetővé teszi az értesítést.

*Megfontolásra érdemes kérdések az e-Privacy Irányelv implementációja során:*

- Az értesítések formáját az e-Privacy Irányelv nem specifikálja. Indokolt lehet ugyanakkor tagállami szinten a lehető legtöbb választási lehetőséget biztosítani az adatkezelők számára az értesítések formáját illetően. Az, hogy az adatkezelő maga választhatja meg a napi működésével és az adatgazdák igényeivel leginkább összhangban levő értesítési módszert, vélhetően jobban motiválni fogja az értesítési kötelezettségek jogszabályszerű teljesítésére és a hatósággal való együttműködésre.
- Ha az értesítés e-mail útján is megtehető, az elektronikus aláírás használatának kötelezettsége az EU-ban is kérdés lehet. Jelenleg az elektronikus aláírás használata még mindig nem annyira elterjedt, hogy indokolt legyen ilyen többletkötelezettséget előírni az e-mailes értesítés során.

## 9. Szankciók

### 9.1 Közigazgatási szankciók

Florida állam jogszabálya szerint[151] az értesítést az adatbiztonsági esemény észlelését, vagy az illetékes hatóságnak az értesítést engedélyező határozatának kézhezvételét követő tíz napon belül elmulasztó félre legfeljebb 500.000 USD összegű bírság szabható ki:

- Amennyiben az értesítésre 30 napon keresztül nem kerül sor, naponta 1.000 USD, ezt követően minden további 30 napos időszakra 50.000 USD vagy ennek arányos része, legfeljebb 180 napig.
- Ha az értesítés 180 napon belül nem történik meg, az értesítést elmulasztó félre legfeljebb 500.000 USD összegű bírság szabható ki.

[150] Ariz. Rev. Stat. § 44-7501 D.
[151] Fla. Stat. § 817.5681 (1) (b)

Az értesítés elmaradása esetén irányadó közigazgatási szankciók adatbiztonsági eseményenként (nem az érintett személyek számának alapulvételével) kerülnek kiszabásra.

Az értesítési kötelezettség elmaradása esetén nem szabhatók ki közigazgatási szankciók, ha az érintett személyes adatok kezelője állami szerv, kivéve, ha az érintett szerv számára a személyes adatokat harmadik személy szolgáltatásnyújtás keretében kezelte, illetve dolgozta fel. Ez esetben a közigazgatási szankciókat az érintett harmadik személy szolgáltatóra kell kiszabni – abban az esetben is, ha a szolgáltató az állami szervet védő jogszabályok miatt nem lesz jogosult a bírság követelésére vagy beszámítására az állami szervvel szemben.

Alaszka állam vonatkozó jogszabálya szerint[152], ha az állami szerv adatkezelő valamely, az érintett állam lakosának személyes adataival kapcsolatban megsérti az értesítési kötelezettségére vonatkozó szabályokat, az adatkezelőre érintett személyenként legfeljebb 500 USD bírság szabható ki, a bírság teljes összege azonban összességében nem haladhatja meg az 50.000 USD-t; az érintett állami szerv ezen felül eltiltható a további jogsértéstől. Ha a nem állami szerv adatkezelő megsérti az értesítési kötelezettségére vonatkozó szabályokat, de a tisztességtelen kereskedelmi gyakorlatra vonatkozó fogyasztóvédelmi jogszabályok szerint nem bírságolható meg, az adatkezelőre érintett személyenként legfeljebb 500 USD bírság szabható ki, és a bírság teljes összege azonban összességében nem haladhatja meg az 50.000 USD-t. Az adatkezelőtől (egyenként és csoportos – *class action* – perindítás útján) kizárólag az 500 USD-t nem meghaladó közvetlen kár megtérítése követelhető, és az ügyvédi költség megtérítése során is kizárólag a közvetlenül felmerült díjak, költségek és károk követelhetők.

*Megfontolásra érdemes kérdés az e-Privacy Irányelv implementációja során:*

- Az egyes EU tagállamokban várhatóan az illetékes adatvédelmi hatóságok, illetve az érintett iparágban illetékes specifikus felügyeleti hatóságok lesznek jogosultak a jogsértés szankcionálására. Az e-Privacy Irányelv ugyanakkor nem határoz meg például türelmi időt, sávos bírságolási lehetőséget, kifejezett bírságolási eseteket vagy bírságmaximumot jogsértés esetén. Eltérő adatbiztonsági események eltérő megítélés alá eshetnek a szankció szempontjából – másképpen indokolt szankcionálni például egy személyes adatokat tartalmazó laptop gondatlan elvesztését vagy az adatkezelés engedélyezett céljainak „egyszerű” megszegését. Tekintettel az adatbiztonsági

[152] Alaska Stat. § 45.48.080

események specifikus jellegére, a bírságolás módszerének meghatározása megfelelő és komplex kidolgozást igényel a hatóságok részéről, és indokolt lehet az érintett szereplők (adatkezelők, fogyasztóvédelmi szervezetek, adatvédelmi-emberi jogi NGO-k) bevonása a folyamatba, például nyilvános konzultációk során.

### 9.2 Az ügyész intézkedései

New York állam vonatkozó jogszabálya szerint[153] ha a legfőbb ügyész (*attorney general*) a rendelkezésére álló megfelelő bizonyítékok alapján úgy véli, hogy az érintett adatkezelő megszegte adatbiztonsági értesítési kötelezettségét, New York állam lakosainak nevében pert indíthat, és kérheti a jogsértés folytatásának megszüntetését. Az illetékes bíróság ítéletében elrendelheti az adatbiztonsági értesítés megtételének elmulasztásával érintett személy kárainak, illetve veszteségeinek megtérítését. Ha a bíróság megállapítja, hogy az érintett adatkezelő szándékosan, vagy súlyos gondatlansággal szegte meg a vonatkozó jogszabályt, a bíróság "büntető jellegű" kártérítést (*civil penalty*) 5.000 USD, vagy elmulasztott értesítésenként tíz dollár értékben, azzal, hogy a második összeg nem haladhatja meg az 150.000 USD összeget. A jogszabályban meghatározott jogorvoslati lehetőségek mellett az egyéb jogorvoslati lehetőségek is gyakorolhatók. A keresetindításra nyitva álló határidő az adatbiztonsági esemény, vagy az eseményről való tudomásszerzés időpontjától számított két év.

Alaszka állam vonatkozó jogszabálya szerint[154] állami szerv adatkezelővel szemben „büntető jellegű" kártérítést az erre illetékes állami szerv (*Department of Administration*) érvényesíthet. Észak-Karolina állam vonatkozó jogszabálya kifejezetten megtiltja a fentiekkel kapcsolatos követelések engedményezését.[155]

Arizona állam vonatkozó jogszabályának[156] rendelkezéseit a legfőbb ügyész érvényesítheti. Az ügyész keresetet indíthat az értesítési kötelezettség szándékos megszegése esetén és jogsértésenként, illetve az adott vizsgálat során feltárt hasonló természetű jogsértések sorozata esetén legfeljebb 10.000 USD összegű "büntető jellegű" kártérítést szabhat ki. Delaware állam vonatkozó jogszabálya szerint[157] szintén a legfőbb ügyész jogosult keresetindításra.

153 N.Y. Gen. Bus. Law § 899-aa 6.
154 Alaska Stat. § 45.48.080
155 N.C. Gen. Stat § 75-65
156 Ariz. Rev. Stat. § 44-7501 H.
157 Del. Code tit. 6, § 12B-104

*Megfontolásra érdemes kérdés az e-Privacy Irányelv implementációja során:*

- Megfontolandó lehet az egyes EU-s tagállamokban az illetékes ügyészt, vagy a fogyasztóvédelmi szervezeteket kifejezetten hasonló keresetindítási joggal felruházni. A gyakorlatban ugyanis nem biztos, hogy az egyes adatgazdák – figyelemmel az ezzel kapcsolatos anyagi és időbeli ráfordításra - külön-külön pert indítanának a jogszabályi kötelezettségeit megszegő adatkezelővel szemben. Tekintettel azonban arra, hogy egy-egy adatbiztonsági esemény akár több száz adatgazda személyes adatát is érintheti, csoportos keresetindítási lehetőség híján az ügyész vagy egy fogyasztóvédelmi szervezet vélhetően hatékonyabban képviselheti érdekeiket.

### 9.3 Jogorvoslati lehetőségek

Washington állam vonatkozó kifejezetten felsorolja az adatgazdák rendelkezésére álló jogorvoslati lehetőségeket.[158]

- Bármely, az adatbiztonsági értesítési kötelezettségekre vonatkozó jogszabályi rendelkezések megszegése által érintett személy polgári per útján kártérítést kérhet.
- Bármely, az adatbiztonsági értesítési kötelezettségekre vonatkozó jogszabályi rendelkezéseket megszegő adatkezelő eltiltható a további jogsértéstől.
- A jogok és jogorvoslati lehetőségek egymás mellett gyakorolhatók.

New Hampshire állam jogszabálya szerint, ha a bíróság a felperes javára ítél, a kártérítési kötelezettség csak a közvetlen károkra terjed ki. Ha a bíróság megállapítja, hogy a jogsértés szándékos volt, vagy az elkövető tudott róla, a károkozó a károk legalább kétszeresét, illetve legfeljebb háromszorosát köteles megtéríteni.[159] Dél-Carolina állam jogszabálya szerint az érintett személy a vonatkozó polgári per során szándékos / tudatos károkozással kapcsolatban kártérítést kérhet; gondatlanság esetén a kártérítési kötelezettség a közvetlen károkra terjed ki. Az érintett személy ideiglenes intézkedés formájában (*injunction*) is kérheti a jogsértő állapot megszüntetését.[160]

158 Wash. Rev. Code § 19.255.010 (10)
159 N.H. Rev. Stat. §§ 359-C:21
160 S.C. Code § 39-1-90 (G)

*Megfontolásra érdemes kérdés az e-Privacy Irányelv implementációja során:*

- Európában az érintett személyek jogai hasonlók, még ha nem is kifejezetten a specifikus jogszabályokban kerülnek meghatározásra, hanem pl. a Ptk.-ban, mint Magyarországon. Az iparági sajátosságokra tekintettel ugyanakkor megfontolandó lehet a kártérítést maximalizálni, az elévülési időt rövidíteni, illetve az egyes, nehezen számszerűsíthető kártípusokat (pl. közvetett károk) kizárni. Egyes iparágakban – például az elektronikus hírközlési szektorban – a gyakorlatban elfogadott a hasonló jellegű felelősségkorlátozás. Ha ez az adatbiztonsági eseményekkel kapcsolatban jogszabály vagy hatósági iránymutatás szintjén is rögzítésre kerülne, az adatkezelők várhatóan nyitottabbak lennének a kártérítési ügyek gyorsabb és hatékonyabb lezárására, akár megállapodás formájában is, megelőzve egy hosszú és minden fél számára költséges kártérítési pert.

### 9.4 Egyéb jogszabályokban meghatározott szankciók

Illinois állam jogszabálya szerint[161] a vonatkozó fogyasztóvédelmi törvény (*Consumer Fraud and Deceptive Business Practices Act*) szerint az adatbiztonsági értesítési kötelezettségekre vonatkozó jogszabályi rendelkezések megszegése a fogyasztókkal szembeni tisztességtelen gyakorlatnak számít. Nem valószínű, hogy az EU tagállamok jogszabályai az adatbiztonsági értesítési kötelezettségekre vonatkozó jogszabályi rendelkezések megszegését tisztességtelen kereskedelmi gyakorlatként fogják meghatározni, és nem is feltétlenül szükséges ez – ez a kategória Európában más típusú és súlyosabb cselekményeknek maradjon “fenntartva”.

## 10. Önszabályozás

Figyelembe véve, hogy az adatbiztonsági kérdéseket és az adatbiztonsági értesítési kötelezettségeket számos társaság belső biztonsági vagy adatvédelmi szabályzatban szabályozza, az USA-ban a legtöbb tagállami jogszabály (pl. Washington[162], Arizona[163], Kalifornia[164], Delaware[165] és Georgia[166] államok jogszabályai) elismeri az ilyen szabályzatok rendelkezéseinek a jogszabályi megfelelőségét. A

161 815 ILCS 530/5 Sec. 20
162 Wash. Rev. Code § 19.255.010 (8)
163 Ariz. Rev. Stat. § 44-7501 E.
164 1798.82. (h) (Cal. Civ. Code)
165 Del. Code tit. 6, § 12B-103
166 Ga. Code §§ 10-1-910

szabályozó hatóságok szintén kibocsáthatnak a jogszabályi rendelkezéseknek való megfelelést kiváltó értesítési eljárásokat.

Florida állam vonatkozó jogszabálya alapján[167] az az adatkezelő, aki

- Saját biztonsági vagy adatvédelmi szabályzata keretében az alkalmazandó jogszabályokkal egyébként összhangban levő adatbiztonsági értesítési eljárást vezetett be; vagy
- Az adatkezelő működésével kapcsolatban illetékes szabályozó hatóság által meghatározott szabályzatokat, illetve eljárásokat alkalmaz,

úgy tekintendő, mint aki az adatbiztonsági értesítési kötelezettségeknek megfelel, ha az érintett személyeket a fenti belső szabályzatokkal vagy az illetékes szabályozó hatóság által meghatározott szabályzatok, illetve eljárások alkalmazásával értesíti.

Arizona állam vonatkozó jogszabálya szerint[168] egyes bűnüldöző hatóságok kötelesek a biztonsági rendszerük megszegése esetén alkalmazandó értesítési eljárást tartalmazó belső szabályzatot bevezetni.

*Megfontolásra érdemes kérdések az e-Privacy Irányelv implementációja során:*

- A gyakorlatban szokásos, hogy az USA-ban működő vállalatok európai leányvállalataikban is hasonló adatbiztonsági értesítési belső szabályzatokat fogadnak el (vagy „lokalizálják" az amerikai szabályzatot). Ennek következtében számos, az EU-ban működő vállalat belső szabályzata tartalmaz ilyen kötelezettséget, még ha ez még nem is kötelező a vonatkozó jogszabályok alapján. Az amerikai példához hasonlóan az EU-ban is érdemes lehet megfontolni a majd elfogadásra kerülő tagállami szabályozásokkal összhangban levő belső szabályzatok készítésének támogatását, illetve azok elismerését, mint a jogszabály által meghatározott értesítési eljárások megfelelő alternatíváját. Az önszabályozó eszközök általában hatékonyabbak, mint a jogszabályok, és gyorsabban adaptálhatók a gyakorlati követelményekhez (új kockázatok, új kérdések) - ez nagyobb védelmet biztosít az adatgazdák számára. Az önszabályozás további előnye, hogy egy

[167] Fla. Stat. § 817.5681 (9)
[168] Ariz. Rev. Stat. § 44-7501 K.

innovatív, ügyfélbarát önszabályozás növeli az adott vállalkozás versenyképességét – erre tekintettel pedig maga a vállalkozás is motiváltabb lesz adatvédelmi gyakorlatának önszabályos útján való fejlesztésére.

- Érdemes lehet az EU tagállamok jogalkotóinak és szabályozó hatóságainak végiggondolni, hogy esetleg mely iparágak szereplői számára lehet indokolt kötelező belső adatbiztonsági értesítési szabályozat készítését előírni, figyelemmel az adott adatkezelő által kezelt adatok „érzékeny" jellegére (pl. pénzügyi szektor, egészségügyi szektor, oktatás).
- Az internetes kereskedelemhez vagy tartalomszolgáltatáshoz hasonlóan megfontolandó lehet önkéntesen alkalmazandó magatartáskódexek és jelentéstételi rendszerek bevezetése is. Az egyes tagállamok adatvédelmi hatóságai aktív szerepet játszhatnak az ilyen szabályok kialakításában. Minden esetben fontos konzultálni a piaci szereplőkkel annak biztosítása érdekében, hogy az újonnan bevezetésre kerülő szabályok gyakorlatiasak és hatékonyak legyenek. Fontos az is, hogy az iparági előírások egységesen kerüljenek kialakításra. Az USA-ban például bizonyos tevékenységek végzése esetén a vállalkozásoknak gyakran kell biztonsági vállalásokat tenniük, mint például a nevadai jog által előírtak szerint, amely kötelezővé teszi a „*Payment Card Industry Data Security Standard*" szabályok használatát. A különböző iparági előírások egységesítése jelentősen megkönnyítheti a több joghatóságban működő vállalkozások számára az összehangolt biztonsági intézkedések megtételét.

## 11. Eltérési lehetőség a jogszabályi rendelkezésektől

Az USA tagállamai jogszabályainak legtöbbje – pl. Washington[169], Alaszka[170] vagy Illinois[171] államok jogszabályai – kifejezetten rögzíti, hogy az adatbiztonsági értesítési kötelezettségek kikényszerítéséről való lemondás sérti a közrendet, ennek következtében semmis és végrehajthatatlan. New York állam vonatkozó jogszabálya[172] rögzíti, hogy az adatbiztonsági értesítésekre vonatkozó jogszabályi rendelkezések kizárólagosak, és elsőbbséget élveznek bármely helyi jogszabály vagy szabályozás rendelkezésével szemben, valamint nem hozható olyan helyi szabályozás, amely a megfelelő állami jogszabállyal ellentétes, vagy annál szigorúbb rendelkezést tartalmaz.

169 Wash. Rev. Code § 19.255.010 (9)
170 Alaska Stat. § 45.48.060
171 815 ILCS 530/5 Sec. 15
172 N.Y. Gen. Bus. Law § 899-aa 9.

Kalifornia államban néhány adatkezelőre - például egészségügyi szolgáltatóra, vagy specifikus egészségügyi jogszabály (Confidentiality of Medical Information Act) hatálya alá tartozó szervre, külön jogszabályban (Financial Code és California Financial Information Privacy Act) meghatározott pénzügyi intézményre, a vonatkozó gépjármű-nyilvántartásból szerződés és az irányadó jogszabály (Vehicle Code) alapján és az ott előírt titoktartási kötelezettségnek megfelelően adatot gyűjtő szervezetre - nem vonatkoznak az általános adatbiztonsági értesítési kötelezettségek; ezen adatkezelőkre specifikus adatvédelmi jogszabályok irányadók.

*Megfontolásra érdemes kérdés az e-Privacy Irányelv implementációja során:*

- Érdemes lehet az EU tagállamok jogalkotóinak és szabályozó hatóságainak végiggondolni, hogy esetleg mely iparágakban lehet indokolt a fentiekhez hasonló specifikus adatbiztonsági értesítési kötelezettségeket előírni, figyelemmel az adott adatkezelő által kezelt adatok „érzékeny" jellegére (pl. pénzügyi szektor, egészségügyi szektor, oktatás).

## 12. Nyilvántartási kötelezettség az e-Privacy Irányelv alapján

Az e-Privacy Irányelv alapján a szolgáltatók olyan nyilvántartást vezetnek a személyes adatok megsértésének eseteiről, amelyek magukba foglalják az ilyen esetek körülményeit, hatását és a korrekciós intézkedéseket is, és elégségesek ahhoz, hogy az illetékes nemzeti hatóságok ennek alapján ellenőrizhessék az adatok megsértésének esetére vonatkozó értesítési kötelezettségnek való megfelelést. A nyilvántartás csak az említett cél eléréséhez szükséges információkat tartalmazza.[173]

*Megfontolásra érdemes kérdések az e-Privacy Irányelv implementációja során:*

- Tekintettel arra, hogy számos szolgáltató végez határon átnyúló – akár európai szintű tevékenységet – fontos lenne biztosítani, hogy a nyilvántartás formája minden országban egységes legyen, megkönnyítve ezzel mind a szolgáltatók, mind a hatóságok feladatát.

[173] e-Privacy Irányelv 4. cikk (4)

- Fontos lenne továbbá tagállami szinten – lehetőség szerint egységesen – meghatározni, hogy ezt a nyilvántartást pontosan hogyan és meddig kell megőrizni, valamint kik jogosultak hozzáférni (pl. adatgazdák az Adatvédelmi Irányelv által biztosított információkérési joguk alapján). Ez szenzitív kérdés lehet, tekintettel arra, hogy az adatbiztonsági eseményekkel és úgy általában, az adatkezelő által alkalmazott adatbiztonsági technikákkal kapcsolatos belső feljegyzések az adatkezelő üzleti titkait képezhetik, melyekkel könnyen vissza lehet élni.

## 13. A szabályozó hatóságok bevonása az e-Privacy Irányelv alapján

A közlések titkosságával kapcsolatos intézkedések következetes végrehajtásának biztosítása érdekében a Bizottság az Európai Hálózat- és Információbiztonsági Ügynökséggel (European Network and Information Security Agency – „ENISA"), a 95/46/EK irányelv 29. cikke alapján létrehozott, az egyének személyes adatok feldolgozása tekintetében való védelmével foglalkozó munkacsoporttal és az európai adatvédelmi biztossal folytatott konzultációt követően műszaki végrehajtási intézkedéseket fogadhat el az e-Privacy Irányelvben említett tájékoztatási és értesítési követelményekre alkalmazandó körülményekre, formátumra és eljárásokra vonatkozóan. Ezen intézkedések elfogadása során a Bizottság bevonja az összes érdekelt felet, különösen annak érdekében, hogy tájékozódjon az új rendelkezések végrehajtását javító, rendelkezésre álló legjobb gazdasági és műszaki megoldásokról.[174]

## 14. Biztonság és integritás a Keretirányelv alapján

A módosított Keretirányelv 13.a cikke ugyancsak tartalmaz egy „specifikusabb" értesítési kötelezettséget, amit érdemes megemlíteni. Eszerint a tagállamok biztosítják, hogy a nyilvános hírközlő hálózatokat szolgáltató és a nyilvánosan elérhető elektronikus hírközlési szolgáltatásokat nyújtó vállalkozások értesítsék az illetékes nemzeti szabályozó hatóságot a biztonság megsértésének és az integritás hiányának minden olyan esetéről, amely jelentős hatással volt a hálózatok, illetve a szolgáltatások működésére. Az adott nemzeti szabályozó hatóság szükség szerint értesíti a többi tagállam nemzeti szabályozó hatóságát és az ENISA-t. Az adott nemzeti szabályozó hatóság tájékoztathatja a nyilvánosságot, illetve a vállalkozásokat erre kötelezheti, amennyiben úgy ítéli meg, hogy a biztonság megsértésének vagy az integritás hiányának nyilvánosságra hozatalához közérdek

[174] e-Privacy Irányelv 4. cikk (5)

fűződik. Az érintett nemzeti szabályozó hatóság a beérkező bejelentésekről és az e bekezdésnek megfelelően tett intézkedésekről évente összefoglaló jelentést nyújt be a Bizottságnak és az ENISA-nak. A Bizottság - a lehető legnagyobb mértékben figyelembe véve az ENISA véleményét - megfelelő műszaki végrehajtási intézkedéseket fogadhat el, így különösen meghatározhatja a bejelentés körülményeit, és a bejelentésre vonatkozóan alaki és eljárási követelményeket állapíthat meg.

## III. GYAKORLATI TANÁCSOK ADATKEZELŐKNEK

Az adatbiztonsági értesítésekkel kapcsolatos (valamint az ezekkel összefüggő általános adatvédelmi) jogszabályoknak és szabályozásoknak való megfelelés biztosítás érdekében az adatkezelőknek az alábbiakat érdemes végiggondolniuk.

### 1. Technikai intézkedések és belső szabályzatok

Nincs egyértelmű információ arról, hogy a gazdasági válság negatívan befolyásolta-e a társaságok IT biztonsággal kapcsolatos költségvetését, vagy továbbra is költenek adatvédelmi intézkedésekre a biztonsági kockázatok csökkentése és a jogszabályoknak való megfelelés erősítése érdekében. Az adatbiztonsági eseményekkel kapcsolatos nyilvánosan elérhető ügyek leírása, és a jogi / pénzügyi következmények alapján nyilvánvaló, hogy a magánszemélyek személyes adatainak védelme fokozott figyelmet igényel. Ennek érdekében a személyes adatokat használó vállalkozásokat ösztönözni kell a személyes adatok megfelelő szintű védelmének biztosítására, beleértve az adatbiztonsági eseményekről szóló értesítési eljárások bevezetését is.
A gyakorlatban az adatkezelők számára az adatbiztonsági értesítések szempontjából a két legfontosabb kötelezettség a következő:

- A személyes adatok technikai védelme céljából megfelelő biztonsági intézkedéseket kell elfogadni.
- Az adatbiztonsági eseményeket az illetékes hatóságok / érintett személyek (adatgazdák) tudomására kell hozni. (Magyarországon egyelőre csak az elektronikus hírközlési szektorban.)

A személyes adatok technikai védelme céljából a megfelelő biztonsági intézkedések elfogadása

nehézséget okozhat, mert úgy tűnik, egyelőre nem lesz egyetlen, a szükséges kötelezettségeket átfogóan megállapító adatvédelmi szabályozás sem az USA-ban, sem az EU-ban – és a jogi kötelezettségek köre folyamatosan szélesedik.[175] Az iparági gyakorlatok és szabványok is folyamatosan fejlődnek, tehát ha nincsenek a jogszabályok vagy a szabályozó hatóságok által kifejezetten meghatározott intézkedések - csupán általános rendelkezések, mint például „ésszerű" vagy „megfelelő" biztonság előírása – az adatkezelőknek nehézkes lesz meghatározni az egyedi megfelelés módját.

A legjobb megoldás, ha az adatkezelők értékelik a lehetséges kockázatokat, ezt követően pedig azonosítják és alkalmazzák a körülmények alapján ésszerűnek mutatkozó technikai és eljárási intézkedéseket a kívánt biztonsági célok elérése érdekében. Ezt követően biztosítani kell az intézkedések és az eljárások folyamatos fejlesztését, figyelemmel kísérését – tekintetbe véve a technikai fejlődést, az új szolgáltatásokat és üzleti modelleket, az ügyfelek igényeit, a fejlődő hatósági és bírói gyakorlatot és a gyakorlatban bekövetkezett adatbiztonsági eseményeket. Természetesen a biztonsági intézkedések magukban foglalják a fizikai védelmet (pl. őrzés, hozzáférés-korlátozás) és az IT intézkedéseket is (pl. tűzfal, behatolás-felismerő szoftver), mind a külső fenyegetésekkel, valamint a gondatlanságból vagy szándékosan kárt okozó belső személyzettel szemben.

Minden adatkezelőnek fontos lehet a vele kapcsolatban álló magánszemélyek (pl. ügyfelek, munkavállalók, szerződő felek) személyes adatai védelmének biztosítása érdekében egy átfogó adatvédelmi és információbiztonsági szabályzat elfogadása is, mely természetesen tartalmazza az adatbiztonsági esemény esetén lefolytatásra kerülő eljárást is. Ennek segítségével a személyes adatokkal kapcsolatos bármely – akár véletlen, akár szándékosan okozott - biztonsági esemény könnyen észlelhető, és az adatkezelő képes lesz azonnal reagálni és megelőzni, illetve minimalizálni a károkat (pl. az adatok jogosulatlan megszerzése és a velük történő lehetséges visszaélés).

### 2. További önkéntes kötelezettségvállalások

Az adatkezelők a jogszabályok vagy belső szabályzatok által megállapított kötelezettségeken túl önként is vállalhatnak biztonsági intézkedéseket, pl. az ebből a szempontból különösen érzékeny kiszervezési (*outsourcing*) szerződésekben, ahol a bizalmas információ vagy személyes adatok jelentős részét a szerződő felek egymás között továbbítják különböző, eltérő adatvédelmi előírásokat alkalmazó joghatóságok között. Az outsourcing kiemelt kockázatokat hordoz a személyes adatok biztonsága

[175] **Data Breach: Security Measures the Law Requires of IT**
http://www.cio.com/article/444545/Data_Breach_Security_Measures_the_Law_Requires_of_IT

szempontjából: 2006-ban például egy outsourcing cégnél Indiában dolgozó munkavállaló állítólag 420.000 USD-t tulajdonított el húsz ügyfélnek a brit HSBC banknál vezetett bankszámlájáról. A lopásra akkor derült fény, amikor az angol ügyfelek a számlájukról 2006 márciusa és májusa között történt, jogosulatlan pénzátutalásokról panaszkodtak.

### 3. Az adatgazdák és az adatkezelők oktatása

A piaci szereplőknek és a szabályozó hatóságoknak egyaránt fontos, hogy az adatgazdákat és az adatkezelők személyzetét megfelelően tájékoztassák az adatbiztonsági eseményekhez kapcsolódó lehetséges kockázatokról (csalások, személyiséglopás) és a szükséges védelmi intézkedésekről. Nagyon jó példa erre az amerikai FTC (Privacy: Tips for Protecting Your Personal Information)[176] vagy akár a Facebook vonatkozó iránymutatása [177]. Az Egyesült Királyságban az ICO jelenleg azt kutatja, hogy miként lehet már általános iskolában oktatni az adatvédelmi szabályok ismeretét.[178]

Az adatbiztonsági értesítések kezelésére vonatkozó belső eljárásokon túl a piaci szereplőknek oktatási programokat kellene bevezetni az adatgazdák (pl. ügyfelek) és saját személyzetük számára az adatbiztonsági eseménnyel érintett adatokkal kapcsolatban felmerülő kockázatokról, valamint az érintett személyek által az esetleges károk megelőzése és csökkentése érdekében teendő lépésekről.

### 4. Közreműködési kötelezettség

A fentieken túlmenően az adatkezelőknek minden esetben közre kell működniük a személyiséglopásokkal, személyazonossággal való visszaélésekkel, csalásokkal, megtévesztésekkel és vonatkozó ügyekkel kapcsolatos ügyfélpanaszok kivizsgálásában, a jogosulatlan kifizetések visszatérítésében, a jogosulatlanul létrehozott bankszámlák törlésében, a meghamisított adatok kijavításában és egyéb ügyekben. Ebből a célból alapvető az együttműködés a nyomozásban és a büntetőeljárásban illetékes hatóságokkal. Az USA Indiana tagállamában kifejezetten ebből a célból került megalapításra az Ügyészség Személyiséglopási Egysége.[179]

---

176 FTC Consumer Alert - **Privacy: Tips for Protecting Your Personal Information** http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt106.shtm

177 **A Guide to Facebook Security** https://www.facebook.com/safety/attachment/Guide%20to%20Facebook%20Security.pdf

178 **ICO wants primary schools to teach data privacy lessons** http://www.computing.co.uk/ctg/news/2105640/ico-primary-schools-teach-privacy-lessons

179 2009 H.B. 1121

## 5. Biztosítás

Az adatbiztonsági eseményekkel kapcsolatos anyagi kockázatok kezelésére magától értetődő megoldás az adatbiztonsági eseményekre kötött biztosítás. Rermészetesen részletesen meg kell vizsgálni az adott biztosítás feltételeit, hogy alkalmazható-e az adatkezelő tényleges tevékenységével összefüggő potenciális káresemények esetén. Egyes biztosítások csak a kötelező adatbiztonsági értesítések költségeinek megtérítésére terjednek ki, míg mások az önkéntes értesítések költségeit, és esetleg az okozott károk megtérítését is magukban foglalják. További kérdés, hogy csak a személyes adatokra, vagy egyéb, az érintett személy azonosítását nem lehetővé tevő adatokra terjed-e ki a biztosítás.

## 6. Az adatbiztonsági értesítések megfogalmazása

Tekintettel arra, hogy az E-Privacy Irányelv egyelőre csak általánosságban rendelkezik az adatbiztonsági értesítések tartalmáról, az adatkezelőknek többek között a következőket kell figyelembe venni az értesítés megfogalmazása során:

- Az értesítés megfogalmazásának illeszkednie kell az érintett cég kommunikációjának stílusába, ugyanakkor megfelelő, könnyen érthető és világosan megfogalmazott információkat kell tartalmaznia a címzettek számára.
- Az értesítés stílusa ugyanakkor rövid és lényegretörő kell legyen (pl. bullet-pointok használatával) - az előfizetők ugyanis hajlamosak figyelmen kívül hagyni a túl részletes, hosszú, nem figyelemfelkeltő formátumban elküldött szolgáltatói értesítéseket.
- Fontos leírni az adatbiztonsági esemény körülményeit. Különbség lehet például egy autóban hagyott laptop ellopása - ahol lehet, hogy a tettesek csak az autót akarták - és egy adatbázis szándékos feltörése között. A részletes információadással megelőzhető, hogy az érintett személyek az egyébként jogos kérdéseikkel erőforrásokat vonjanak el az adatkezelőtől az esemény megoldása során.
- Hatósági iránymutatások hiányában a különböző adatbiztonsági szolgáltatók által kibocsátott ajánlásokat is célszerű figyelembe venni.[180]

[180] Például: **How to Inform Customers of a Data Breach** - https://infosecisland.com/blogview/15071-How-to-Inform-Customers-of-a-Data-Breach.html

A jogszabályok nem írnak elő kifejezett felkészülési kötelezettségeket egy esetleges adatbiztonsági eseményre, pedig ez feltehetőleg számos adatbiztonsági eseményt megakadályozhat. Ilyen intézkedés lehet például:

- Előzetesen meg kell vizsgálni, hogy mit lehet tenni az adatbiztonsági események megelőzése érdekében, és mi lehet egy lehetséges adatbiztonsági esemény gyakorlati hatása, figyelembe véve a technológiai változásokat is (*risk impact assessment*). Pontosan meg kell vizsgálni, hogy milyen információ sérülhet, milyen jogosulatlan tevékenység vagy véletlen esemény következtében, milyen személyes adatokat (pl. jelszavakat) kellene kiemelt gondossággal védeni (pl. titkosítás).
- Ki kell jelölni egy vagy több, az adatbiztonsági esemény esetén eljáró / az érintett személyekkel kapcsolattartó személyt (*incident response team, technical response team*) és pontosan meg kell határozni az esemény bekövetkezésekor lefolytatásra kerülő eljárást (pl. határidők, lépések, cégen belüli kommunikációk, cégen kívüli kommunikációk) (*recovery/contingency plan*).
- Megfelelő, hatályos elérhetőséggel kell rendelkezni az esetlegesen érintett személyekhez, hogy az értesítések gyorsan és hatékonyan elküldésre kerülhessenek.
- Az eseményt követően azonosítani kell az okokat és megoldást keresni a jövőre nézve a hasonló helyzetek megelőzése érdekében. Azonosítani kell, milyen következményei voltak az eseménynek (pl. személyiséglopás, jogosulatlan pénzügyi tranzakciók). Meg kell vizsgálni, hogy szükséges-e az érintett személyeken kívül más szerződő partnereket is értesíteni.
- Fel kell készülni az illetékes adatvédelmi hatóság esetleges helyszíni vizsgálatára is.
- Fontos a munkavállalók megfelelő oktatása az adatkezelési gyakorlattal kapcsolatban („*data security wisdom*”), többszöri alkalommal, feladatkörönként eltérően, gyakorlati példákon keresztül. Az oktatás eredményét természetesen megfelelően dokumentálni és ellenőrizni kell. Fontos az események időben való felismerése (tekintettel a haladéktalan értesítési kötelezettségre).
- Az adatbiztonság nem csak technikai kérdés, és egy adatbiztonsági eseményt nem lehet megfelelően kezelni kizárólag IT eszközökkel: elengedhetetlen az egyes (személyes adatokat kezelő) területek (pl. HR, marketing) és az érintett tanácsadók (IT, jog)

együttműködése is.

## IV. VÁRHATÓ SZABÁLYOZÁSI FEJLEMÉNYEK

Elöljáróban érdemes megjegyezni, hogy a jogszabályon alapuló kötelező adatbiztonsági értesítési kötelezettség gyakorlati működőképességének megítélése még mindig ellentmondásos. Az üzleti hírnév védelme az adatkezelőket adatbiztonsági megoldásaik javítására, és ezzel az adatbiztonsági helyzetek megelőzésére indíthatja, ugyanakkor fennáll a veszélye annak, hogy az adatbiztonsági értesítések növekvő száma miatt a nyilvánosság kevésbé lesz érzékeny az adatbiztonsággal összefüggő veszélyekre.

### 1. Várható fejlemények az USA-ban

Amint azt a II. Fejezetben kifejtésre került, az USA-ban az adatbiztonsági helyzetekkel kapcsolatos értesítési kötelezettséget az egyes tagállamok jogszabályai szabályozzák, noha vannak javaslatok a kérdés szövetségi szinten történő szabályozására.[181] A tagállamonként különböző adatbiztonsági értesítési szabályozás gyakorlati alkalmazása az USA-ban is számos nehézséget okoz. Különböző értesítési okok, eltérő definíciók és címzetti kör, változó határidők, specifikus jogorvoslati lehetőségek - mind-mind olyan akadály, ami jelentősen megnehezíti a tagállami határokon átnyúló adatbiztonsági értesítések gyors és hatékony megvalósítását. A szövetségi szintű szabályozás még várat magára – jelenleg több különböző törvényjavaslat megvitatása is folyamatban van, viszont minden érintett szereplő tisztában van azzal, hogy az összes tagállamra kiterjedő adatbiztonsági értesítési szabályozásra van szükség. Sőt, akár az USA joghatóságán kívüli területekre kiterjedően is: ha az érintett tagállamok lakosai külföldön dolgoznak, az értesítési eljárás a jogszabályokban meghatározott időnél tovább tarthat.

További változások – részletszabályok – várhatók a pénzügyi szektorban. A jelenlegi szabályok jelentős védelmet biztosítanak az ügyfelek számára arra az esetre, ha például valaki visszaélne bankkártyájukkal, ugyanakkor további részletes szabályokat igényel az ügyfelek számára a hamis pénzügyi terhelések bejelentése, töröltetése, a jogosulatlanul átutalt összegek visszaszerzése, az adatbiztonsági esemény által érintett bankkártyák lecserélése. Elvárható lehet az is az adatkezelőktől, hogy ha az adatbiztonsági esemény az ő gondatlanul eljárásuk következménye, az ügyfeleknek hitelinformációs-rendszer figyelő szolgáltatásokat kínáljanak fel. Korábban már említésre került, hogy

[181] http://www.jdsupra.com/post/documentViewer.aspx?fid=b303e848-0250-42a5-ba01-3a5ef63a22a6

az adatbiztonsági helyzetek igen költségesek az adatkezelők számára: a pénzügyi szektorban jellemzően ezeket a költségeket továbbhárítják a kártyabirtokosokra magasabb díjak vagy késedelmi kamatok formájában.[182]

Egy jellemző példa a határokon átnyúló adatbiztonsági helyzet által felvetett gyakorlati problémára az USA-ból: 2005 februárjában például a ChoicePoint, egy, több millió ügyfél személyes és pénzügyi adatát feldolgozó társaságnál merült fel adatbiztonsági esemény, amelynek következtében közel 145.000 ember személyes adata került egy bűnszervezet kezébe. A társaság az adatbiztonsági helyzetről először (a kaliforniai jogszabályoknak megfelelően) csak a kaliforniai lakosokat értesítette, és csak később tette közzé, hogy más állambeli lakosok is érintettek lehetnek – a késedelem következtében az utóbbi érintettek nagyobb kockázatnak voltak kitéve. [183]

## 2. Várható fejlemények az EU-ban

Az EU-s szabályozás hiányosságait felismerve az Európai Bizottság 2011. július 14-én nyilvános konzultációt hirdetett az adatbiztonsági értesítésekkel kapcsolatos eljárásokkal kapcsolatban.[184] A konzultáció célja, hogy az érintett személyek – piaci szereplők, szabályozó hatóságok, fogyasztóvédelmi szervezetek – elmondhassák az eljárásokkal kapcsolatos gyakorlati tapasztalataikat és felvethessék az általuk fontosnak tartott szabályozási kérdéseket.

A konzultációs dokumentum szerint különösen fontos tisztázni például a következőket:

- A „*hátrányosan érinti*” kifejezés pontosabb meghatározása (gyakorlati példákkal), valamint az előfizetők és egyéb érintett személyek érintettségének szétválasztása.
- A „*megfelelő technikai védelmi intézkedések*”, valamint értékelési módjuk meghatározása gyakorlati példákon keresztül.
- Ha a szabályozó hatóság kötelezi a szolgáltatót az előfizetők értesítésére – mik a hatóság beavatkozásának körülményei és az alkalmazott határidők?

---

182 A pénzügyi szektor adatbiztonsági értesítési szabályaival kapcsolatos javaslatokról részletesen lásd: Anita Ramasastry: **Heartbreak over Heartland: Why Prosecution for Data Breaches Isn't Enough** http://writ.news.findlaw.com/ramasastry/20090904.html

183 A felvetett problémáról lásd: Anita Ramasastry: **A Federal Court Dismisses a Suit Based on a Threat of Identity Theft and an Extortion** http://writ.news.findlaw.com/ramasastry/20100127.html

184 **ePrivacy Directive: circumstances, procedures and formats for personal data breach notifications - Public consultation** http://ec.europa.eu/information_society/policy/ecomm/doc/library/public_consult/data_breach/ePrivacy_databreach_consultation.pdf

- A „*bűnüldöző hatóságok jogos érdekei*” körének és az „*indokolatlan késedelem nélkül*” fogalmának pontos meghatározása.
- Az értesítési csatornák módjának meghatározása (pl. e-mail vagy levél).
- Az adatbiztonsági eseményekkel kapcsolatos nyilvántartás formája és elemei.
- Hogyan kell a Keretirányelv 13.a cikke szerinti értesítési kötelezettséget és az E-Privacy Irányelv szerinti adatbiztonsági értesítési kötelezettséget párhuzamosan alkalmazni?
- Mik a határon átnyúló adatbiztonsági eseményekkel kapcsolatos gyakorlati tapasztalatok?

## 3. A szabályozó hatóságok szerepe

A legtöbb EU-s országban az adatbiztonsági eseményekkel kapcsolatos kötelezettségek megszegését nemcsak az ügy körülményeinek a hatóság által történő nyilvánosságra hozatalával szankcionálják (amely az adatkezelő piaci hírnevére lehet negatív befolyással), hanem komoly bírságokkal is. Amint az a Bevezetésben említetésre került, az Egyesült Királyság adatvédelmi hatósága például komoly bírságokkal igyekszik biztosítani az adatvédelmi megfelelőséget.

Megállapítható tehát, hogy a szabályozó hatóságok leghatékonyabb eszköze a bírság. Fontos azonban a „szabályozott” adatkezelők és a szabályozó hatóság megfelelő, partneri viszonya. A szabályozó hatóságoknak ismerniük kell a gyakorlatot - vagyis például az adatkezelők IT biztonsági gyakorlatait és szabályzatait - annak érdekében, hogy megfelelően kezeljék az adatgazdák esetleges panaszait és a gyakorlatban alkalmazható ajánlásokat és állásfoglalásokat bocsássanak ki. A jó kapcsolat az adatkezelőkkel már csak azért is fontos, mert együttműködésük (pl. információátadás) elengedhetetlen egy-egy hatósági vizsgálat gyors és hatékony lefolytatásához.

A Bevezetésben említett egyik esetben - amikor egy mobiltelefon-társaság munkavállalói állítólag az előfizetői szerződésekkel kapcsolatos személyes adatokkal kereskedtek - az ICO vonatkozó sajtóközleményének kibocsátását számos kritika érte[185]. Az érintett cég versenytársai rögtön sajtóközleményben zárták ki érintettségüket, így a fogyasztók azonosíthatták az elvileg titkos eljárásban érintett céget. Tanulság: az adatbiztonsági esemény folyamatban lévő vizsgálatával

[185] **Regulators need to build bridges, not burn them** http://www.thelawyer.com/regulators-need-to-build-bridges-not-burn-them/1002773.article

kapcsolatos információk nyilvánosságra hozatala az adatkezelőket meggátolhatja az ICO-val való együttműködésben. Annak ellenére, hogy fontos figyelembe venni az iparági szereplők érdekeit is, ezzel együtt fontos elkerülni a „*regulatory capture*" vagy „*regulatory paralysis*"[186] néven emlegetett jelenséget, vagyis az adatkezelő és a hatóság közötti viszonnyal kapcsolatos indokolatlan aggodalmat; az az elsődleges, hogy a szabályozó hatóságok ragaszkodjanak az adatbiztonsági értesítésekkel kapcsolatos jogszabályi kötelezettségeik betartásához.

*A szerző ügyvéd, a CMS Cameron McKenna LLP budapesti irodájának munkatársa. Az írással kapcsolatos kérdéseket, észrevételeket a marton.domokos@cms-cmck.com vagy a marton.domokos@gmail.com címre várja.*

*A várható adatvédelmi szabályozási fejleményekről érdemes még elolvasni a következő beszélgetést:*

**„Az adatvédelem helyzete 2012-től"**

http://www.hvgorac.hu/sites/portal/interju_oldal.html

[186] Az ICO eljárásáról részletesen: **In defence of the ICO (and regulators)** http://charlesrussell.wordpress.com/2009/12/04/in-defence-of-the-ico-and-regulators/