PÁZMÁNY 1635
alapítva

Pázmány Law Working Papers

2016/27

Szabó Endre Győző

Az Európai Unió általános adatvédelmi rendeletének egyes kérdéseiről II.

Beépített és alapértelmezett adatvédelem - Adatvédelmi incidensek bejelentése

Pázmány Péter Katolikus Egyetem
Pázmány Péter Catholic University Budapest
http://www.plwp.eu

Az Európai Unió általános adatvédelmi rendeletének egyes kérdéseiről II.

Beépített és alapértelmezett adatvédelem

Adatvédelmi incidensek bejelentése

Az Európai Unió új adatvédelmi szabályai

Az Európai Bizottság 2012-ben nyújtotta be javaslatát egy új adatvédelmi keretre nézve. Az Európai Unió két társ jogalkotó szerve négy év tárgyalás után hagyta jóvá a két jogalkotási aktusból álló csomagot:

- Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről

- Az Európai Parlament és a Tanács (EU) 2016/680 irányelve (2016. április 27.) a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről.

A több részletben megjelenő írások sorában az első jogalkotási aktust, az általános adatvédelmi rendeletet [1] vizsgáljuk. A sorozat első részében a jogalkotói célokkal és kiemelten az adatok hordozhatóságával, mint új érintetti jogosultsággal, valamint az előzetes adatvédelmi hatásvizsgálattal foglalkoztunk. Jelen írás tárgya két új alapelv, a beépített és az alapértelmezett adatvédelem elve, valamint az adatvédelmi incidensek kötelező bejelentése az adatvédelmi felügyeleti hatósághoz.

[1] A rendeletet gyakran GDPR-ként (General Data Protection Regulation rövidítése) is említik, akár magyar nyelvű dokumentumokban, illetve közegben is.

Beépített és alapértelmezett adatvédelem [2]

A két elv rögzítése a rendeletben régóta megfogalmazott elvárás alapján történt. Az új elvek nem járnak új kötelezettségek bevezetésével, hanem inkább annak értelmezésére szolgálnak, hogy milyen módon kell az egyébként már létező kötelezettségeket végrehajtani. Az európai adatvédelmi hatóságokat tömörítő az adatvédelmi irányelv 29. cikke alapján létrehozott Munkacsoport 3/2010. számú véleményében részletesen mutatta be az elszámoltathatóság[3] elvét, konkrét javaslatot fogalmazva meg annak kodifikációjára nézve.

Az elszámoltathatóság elvéhez való kapcsolódásról

Az elszámoltathatóság elvének lényege kettős: egyrészt azt várja el az adatkezelőtől, hogy kialakítsa azokat a belső szabályokat, folyamatokat, mechanizmusokat, amelyek a rendeletből fakadó kötelezettségek teljesítéséhez szükségesek, másrészt a megfelelés bemutatásának képességét várja el. Azt tehát, hogy az adatkezelő a hatóság kérésére be tudja mutatni, hogy milyen módon jár el az egyes, rá háruló kötelezettségek teljesítése során. A rendelet 5. cikk (2) bekezdése rögzíti az elszámoltathatóság elvét.

A beépített és az alapértelmezett adatvédelem elve illeszkedik az elszámoltathatóság elvéhez, annak is inkább az első eleméhez. Mind a kettő esetében a megfelelő technikai és szervezési intézkedések megtétele az elvárás, amelynek személyre szabottan kell megtörténnie, és az adatkezelés sajátosságaihoz kell igazodnia.

A beépített adatvédelem elve

A környezetvédelemből ismert legjobb elérhető technológia elve[4] ismerhető fel tulajdonképpen a beépített adatvédelem elvében. Az adatkezelő köteles figyelembe venni a tudomány és a technológia állását, a megvalósítás költségeit, az adatkezelés jellegét, hatókörét, körülményeit és céljait az egyik oldalon, a másik oldalon pedig a természetes személyek jogaira jelentett kockázatokat kell azonosítania és elemeznie. Mindezek fényében határozható meg, hogy az adott szervezeten belül, az adott adatkezelést a feltárt körülmények között miként lehet a beépített adatvédelem elvárásának megfelelően alakítani. Az intézkedések célja a rendeletnek való megfelelés, az alapelvek érvényesítése és az érintett jogainak védelméhez szükséges garanciák megteremtése.

Az alapértelmezett adatvédelem elve

Az alapértelmezett adatvédelem középpontjában az az elvárás áll, hogy csak olyan személyes adatok kezelésére kerüljön sor, amelyek az elérni kívánt cél szempontjából szükségesek. Az alapelv jelent mennyiségi korlátot is, de garanciája annak is, hogy az adatok kezelésének mértékére, tárolásuk időtartamára és hozzáférhetőségére nézve is megfelelő intézkedéseket alkalmaz az adatkezelő.

[2] A két elvet a rendelet 25. cikke rögzíti, a (78) preambulum bekezdés kapcsolódik a szabály értelmezéséhez.
[3] Az angolszász jogi terminológiában pontos tartalom társul az accountablity elvhez, azonban sok más tagállam jogi terminológiájában nehéz a pontos megfelelőjét megtalálni. A rendelet elfogadásával ennek az elvnek a tartalma is rögzítést nyert.
[4] Best available technology (BAT)

Kiemeli a jogalkotó azt a célt, hogy alapértelmezés szerint az adatok nem válhatnak meghatározatlan számú személy számára hozzáférhetővé. Az érintett várakozása is szerepet játszik ennek az elvnek a megvalósításában: ha az érintettet meglepetésként éri az adat kezelése, akkor ez erősíti annak feltevését, hogy az alapértelmezett adatvédelem elve nem érvényesült, vagy legalábbis az adatkezelő és az érintett más várakozásokkal vált az adott jogviszony részesévé. Az alapértelmezett adatvédelem elvének érvényesítése esetén az érintett, a felhasználó olyan környezettel találkozik, amelyben a magánszférája, valamint személyes adatai védelmére nézve a lehető legkedvezőbb feltételek fogadják, és nem kíván semmilyen beállítást, erőfeszítést a felhasználótól, hogy ez az állapot elérhető legyen.

Adatvédelmi incidens bejelentése[5]

Az adatvédelmi incidenst azonos szakaszban szabályozza a rendelet, mint az adatbiztonságot, mégsem adatbiztonsági, hanem adatvédelmi incidens lett a jogalkotó által választott végleges szakkifejezés

Nem új a fogalom maga, a szabályozás, az eljárás azonban sok újdonságot hoz a 2015. október 1-jétől hatályos magyar szabályozáshoz [6] képest is.

Az incidensről való nyilvántartások és értesítések három szintjét különböztetjük meg: az első szinten az adatkezelő házon belül nyilvántartást vezet az incidensekről annak érdekében, hogy azt szükség esetén a hatóság rendelkezésére tudja bocsátani egy ellenőrzés keretében. A második szint akkor valósul meg, amikor az adatkezelő a hatóságot is tájékoztatja az incidens körülményeiről a lent leírt módon és adattartalommal. A harmadik szintet az jelenti, amikor az adatkezelő az érintetteket, illetve a nyilvánosságot tájékoztatja az incidens körülményeiről.

Az incidensek kötelező regisztrációja révén elkerülni kívánt kockázatok

A jogalkotó szándéka szerint az incidensek bejelentése révén el lehet kerülni, illetve enyhíteni lehet azokat a kockázatokat, amelyek a következőkben nyilvánulnak meg: a természetes személyeket érhető fizikai, vagyoni és nem vagyoni károk, az, hogy személyes adataik felett elveszíthetik a rendelkezésüket, jogaikban korlátozhatják őket, személyazonosság lopás, vagy személyazonosság visszaélés áldozatai lehetnek, az álnevesítést jogosulatlanul feloldhatják, a jó hírnevük sérülhet, a szakmai titoktartás alá eső adatok elveszíthetik bizalmas jellegüket, vagy egyéb gazdasági vagy szociális hátrányt szenvedhetnek. Az adatvédelmi intézkedés tehát mindezeket a lehetséges társadalmi következményeket szem előtt tartva érvényesítendő.

Az incidenst követő intézkedések

[5] Az intézményt a rendelet 33-34. cikke szabályozza, ide kapcsolódik továbbá a (85)-(88) preambulum bekezdés.
[6] A háromszintű nyilvántartási, illetve tájékoztatási szint közül az első már a 2015. októberi módosítás előtt is szerepelt az Infotv-ben. A törvény 7. § (5) bekezdés f) pontjában előírta, hogy a személyes adatok automatizált feldolgozása során az adatkezelő és az adatfeldolgozó további intézkedésekkel biztosítja azt, hogy az automatizált feldolgozás során fellépő hibákról jelentés készüljön.

A lehetséges hátrányok súlyosak, ezért a jogalkotó gyors intézkedést vár az adatkezelőtől a helyzet orvoslása érdekében. A határidő a tudomásszerzéstől számított 72 óra, az adatkezelő ennyi idő alatt jelenti be az incidens körülményeit az adatvédelmi hatóságnak. Ha nem tud mindent egyszerre bejelenteni, akkor lehetőség van arra, hogy később részletekben történjen meg a bejelentés. Akár késedelembe esik, akár részletekben szolgáltatja az adatokat a határidőn túl, az igazolás terhe az adatkezelőn van.

Akkor is az adatkezelőnek kell igazolnia a körülmények fennállását, ha az incidens valószínűsíthetően nem jár kockázattal az érintettek jogaira nézve. Ebben az esetben ugyanis nem áll fenn az adatvédelmi hatóság felé bejelentési kötelezettség.

Az adatfeldolgozó felelősségét kiemeli a rendelet, amikor úgy rendelkezik, hogy az általa észlelt incidenst indokolatlan késedelem nélkül jelenti az adatkezelőnek. Amennyiben az adatkezelő először az adatfeldolgozótól értesül az incidensről, akkor a 72 órás határidő ekkor kezdődik.

Az adatvédelmi felügyelő hatóság értesítése

A hatósághoz eljuttatott bejelentésben az incidens körülményeit részletesen be kell mutatni, így ki kell térni az incidens jellegére, az érintettek kategóriáira és hozzávetőleges számukra, be kell mutatni az adatok kategóriáit és számát, meg kell adni a kapcsolattartó vagy a megbízott adatvédelmi tisztviselő nevét és elérhetőségét, ismertetni kell az incidens valószínűsíthető következményeit, az orvoslására tett vagy tervezett intézkedéseket, továbbá a hátrányos következmények enyhítését célzó intézkedéseket.

Az adatkezelő a hatóság értesítésétől függetlenül is köteles az incidensekről belső nyilvántartást vezetni. Ennek tartalmára nézve a rendelet csupán az incidenshez kapcsolódó tényeket, annak hatásait és az orvoslására tett intézkedéseket említi. A nyilvántartás célja, hogy adott esetben a hatóság ellenőrizhesse a rendeletnek való megfelelést az adatkezelőnél.

Az érintettek tájékoztatása

Ha az incidens valószínűsíthetően magas kockázattal jár az érintettekre nézve, akkor az adatkezelő indokolatlan késedelem nélkül világos és közérthető tájékoztatást ad legalább az incidens jellegéről, az adatvédelmi tisztviselő elérhetőségéről és a valószínűsíthető kockázatokról, továbbá a következmények orvoslására tett vagy tervezett intézkedésekről. Kiemelendő, hogy az érintetteknek adandó „indokolatlan késedelem” nélküli tájékoztatás független a hatóság felé érvényes 72 órás határidőtől.

Az adatkezelő mentesül az érintettek tájékoztatásának kötelezettsége alól, amennyiben az adatbiztonsági intézkedéseknek köszönhetően az elvesztett adatok mások számára értelmezhetetlenek, vagy az érintetteket fenyegető kockázat valószínűsíthetően nem valósul meg, továbbá akkor sem, ha az érintettek tájékoztatása aránytalan erőfeszítéssel járna. Ebben az utolsó esetben a nyilvánosság tájékoztatása kiváltja az érintetteknek eljuttatandó közléseket.

Az adatvédelmi felügyelő hatóság feladatai

Az adatvédelmi hatóság fogadja az adatvédelmi incidensekről szóló értesítéseket. Ez számos európai adatvédelmi hatóságnál, így a magyarnál is felkészülést igényel, ugyanis új, eddig ismeretlen feladatról

van szó. Az ügyek jellegénél fogva érdemi és gyors értékelést kell a hatóság oldalán elvégezni, amelyet várhatóan informatikai és jogi felkészültséggel egyfajta ügyeleti rendszerben lehet majd ellátni. Ha a hatóság értékelése szerint az incidens valószínűsíthetően magas kockázattal jár, és a megtett intézkedések ezek orvoslására nem elegendőek, elrendelheti az érintettek tájékoztatását, amennyiben erre még nem került sor. Értékelésében a hatóság azt is megállapíthatja, hogy az érintettek tájékoztatása valamely leírt körülmény teljesülése révén nem szükséges.

A (88) preambulum bekezdés utal az adatvédelmi incidensről szóló eljárások részletes szabályaira. Az Európai Adatvédelmi Testület a rendelet alapján saját kezdeményezésre, illetve valamely tagjának vagy a Bizottságnak a kérésére megvizsgálja a rendelet alkalmazását érintő kérdéseket, és a rendelet egységes alkalmazásának elősegítése érdekében iránymutatásokat, ajánlásokat és legjobb gyakorlatokat tesz közzé. A Testület ennek megfelelően az adatvédelmi incidens és az indokolatlan késedelem tényének megállapítására, valamint azokra a konkrét körülményekre nézve, amelyek alapján az incidens bejelentésének kötelezettsége fennáll, az említett dokumentumokat bocsáthatja ki. Ehhez hasonlóan az adatvédelmi incidens valószínűsíthetően magas kockázatát jelző körülmények terén is kibocsáthat iránymutatásokat, ajánlásokat és legjobb gyakorlatokat.

Több tagállamban van már általános bejelentési kötelezettség (így Írországban, Hollandiában), ezek tapasztalatai fontosak lesznek a közös európai uniós iránymutatások kialakítása során.