HADMÉRNÖK

XIII. Évfolyam 3. szám – 2018. szeptember

# A SZEMÉLYES ADATVÉDELMI MEGFELELÉS ELLENŐRZÉSE ÉS A BEKÖVETKEZETT ADATVÉDELMI INCIDENSEK KEZELÉSÉNEK FELADATAI AZ UNIÓS SZABÁLYOZÁS KERETEIN BELÜL

## CONTROL OF PERSONAL DATA PROTECTION CORRECTIONS AND TASKS OF MANAGING DATA PROTECTION INCIDENTS UNDER THE UNION REGULATORY FRAMEWORK

MÓGOR-KRÓZSER Terézia

ORCID: 0000-0002-0272-1985

mogor.krozser.terezia@uni.nke.hu

***Absztrakt***

*A publikáció rövid áttekintést ad az Európai Parlament és a Tanács 2016/679 rendelete (a továbbiakban: GDPR /Rendelet) bevezetésével, gyakorlati megvalósításával kapcsolatos egyes kérdésekről. A cikk bemutatja a személyes adatvédelmi megfelelés ellenőrzésének lehetőségeit és a bekövetkezett incidensek kezelésének legfontosabb feladatait. A publikáció révén szeretném kihangsúlyozni, hogy az adatvédelmi jogszabályoknak való megfelelőség alapvető eszköze az ellenőrzés, melynek alkalmazásával lehetővé válik a feltárt hiányosságok korai kezelése. Mindez hozzájárulhat az adatvédelmi mulasztások bekövetkezésének megelőzéséhez vagy a bekövetkezett incidensek számának csökkentéséhez.*

**Kulcsszavak:** *adatvédelmi szabályozás, személyes adatkezelés, adatvédelmi megfelelés ellenőrzése, incidenskezelés.*

***Abstract***

*This publication gives a brief overview of certain issues related to the implementation and practical implementation of Regulation 2016/679 of the European Parliament and of the Council (hereinafter the "GDPR"). The article describes the possibilities of controlling personal privacy compliance and the most important tasks of managing incidents. Through the publication, I would like to emphasize that compliance with data protection legislation is a fundamental tool for control, which will enable the early management of detected shortcomings. This can contribute to preventing the occurrence of data breaches or to reduce incidents.*

***Keywords:*** *data protection, personal data management, compliance with data protection compliance, incident management.*

A kézirat benyújtásának dátuma (Date of the submission): 2018.07.08.
A kézirat elfogadásának dátuma (Date of the acceptance): 2018.09.26.

## BEVEZETÉS

Az utóbbi évtizedek technikai és technológiai fejlődése és az elmúlt két évtizedben létrejött digitális, vezeték nélküli és vezetékes kommunikációs módok lényegesen hozzájárulnak ahhoz, hogy az emberek személyes adataikat, információikat napi rendszerességgel és bátrabban osztják meg, mint korábban. Ez a korábbinál nagyobb veszélyeket hordoz személyes adatainkkal kapcsolatos védelem vonatkozásában.

Az Európai Parlament és Tanács (EU) 2016/679 számú rendelete (a továbbiakban GDPR[1]/Rendelet) 2018. május 25-től kötelezően alkalmazott szabályozás, amely nem csak visszaadja a polgároknak a személyes adataik feletti ellenőrzést, hanem számos lehetőséget biztosít a vállalkozások terén is, így az európai polgárok és vállalkozások lehetőséget kapnak arra, hogy a digitális gazdaság nyújtotta előnyöket maradéktalanul kihasználhassák.

## MIÉRT VOLT SZÜKSÉGES AZ UNIÓS ADATVÉDELMI REFORM, MILYEN ELŐNYÖKKEL JÁR?

A korábbi adatvédelmi szabályok[2] bevezetése óta több mint 20 év telt el a GDPR megalkotóinak az is célja volt, hogy a kis – és középvállalkozások adminisztrációs terheit csökkentsék, továbbá törekedtek arra, hogy a jogszabály kövesse a „kockázatalapú megközelítést”[3].

Szakértői anyagok támasztják alá, hogy a GDPR jelentős változást hoz azáltal, hogy egy, az Európai Unió egész területén egységesen alkalmazandó adatvédelmi szabályozást ír elő. Az új szabályozás biztosítja, hogy a vállalkozásoknak 28 jogszabály helyett csupán egyet kell alkalmazniuk, ami az adminisztratív terhek egyszerűsítése mellett a pénzügyi kiadások mértékét is csökkentheti[4]. Becslések szerint az új szabályok alkalmazása megközelítőleg 2,3 milliárd euro hasznot is hozhat.[1]

A financiális kiadások csökkenése mellett az új rendelet egyrészt nagyobb betekintést és jogokat biztosít a magánszemélyek részére adataik kezelésével kapcsolatban, másrészt a cégek ez irányú kötelezettségeit növeli, a mulasztásokat pedig az eddiginél jelentősebb pénzbüntetéssel sújtja. [2]

## MIT ÉRDEMES TUDNI AZ ADATVÉDELMI MEGFELELÉS ELLENŐRZÉSÉNEK LEHETŐSÉGEIRŐL?

Akár a bírság, akár a kártérítési felelősség veszélye miatt az egyes vállalkozásoknak érdemes a GDPR előírásaihoz igazítaniuk a személyes adatokkal kapcsolatos működésüket, rendszereiket, folyamataikat. Ebben a fejezetben bemutatom annak lehetőségeit, hogy milyen módon ellenőrizhető saját vállalkozásunk adatvédelmi megfelelése.

Elsőként érdemes figyelmet fordítani az adatkezelésünk átvilágítására úgy, hogy feltérképezzük az összes adatbázisunkat. A teljesség igénye nélkül szeretnék kiragadni néhány fontos példát [3]:

---

[1] General Data Protection Regulation

[2] Az információs önrendelkezési jogról, és információszabadságról szóló 2011. évi CXII. törvény (Infotv.). és a 95/46/EK adatvédelmi irányelv.

[3] Ha a GDPR előírja egy vállalkozás számára az érintett jogait és szabadságait érintő kockázat felmérését, akkor a kockázat valószínűségét és súlyosságát objektív értékelés alapján, az adatkezelés jellegének, hatókörének, körülményeinek és céljainak függvényében kell meghatározni.

[4] A korábbi szabályozás alapján ugyanis az a cég, aki több tagállamban szeretett volna árukat eladni vagy szolgáltatást nyújtani, mindenhol meg kellett, hogy feleljen a helyi adatvédelmi szabályozásnak és hatósági követelményeknek.

- Adatkezelői szinten vizsgálni kell a munkatársak személyes adatainak munkaviszonyból eredő kezelését. Ide sorolható a munkahelyi telefonhasználat vagy e-mail tartalmak ellenőrzése, továbbá a beléptető rendszer működtetése, alkohol-drogteszt vagy a munkaviszonnyal kapcsolatos adattovábbítások.
- A legtöbb vállalkozás végez toborzási tevékenységet, mely során természetes személyek személyes adatait kezeli. A Rendelet követelményeinek értelmében az érintetteket5 előzetesen tájékoztatni kell az adatkezelés körülményeiről. Hozzájárulásuk megadása előtt tudniuk kell azt, hogy személyes adataikkal mi történik: pontosan ki kezeli, feldolgozza-e, ha igen milyen célból teszi azt, kik férnek hozzá az érintett személyes adataihoz? Szeretném kihangsúlyozni, hogy hozzájárulás nélkül még az illetékes személy nyilvános közösségi profiljáról sem gyűjthető adat.
- Adatvédelmi szempontból aggályos lehet a személyazonosító iratok másolata. Amennyiben a másolást jogszabály nem írja elő, ez a gyakorlat szükségtelen adatkezelésnek minősül, így jogellenessé válik ez a tevékenység.
- Vizsgáljunk meg egy olyan vállalkozást is, amely közvetlen üzletszerzésre is támaszkodik. Ebben az esetben is számos kérdést kell tisztázni. Lényeges, hogy cégeket vagy magánszemélyeket keres meg, milyen formában éri el az érintetteket, mert más szabályok vonatkoznak az e-mailes, a postai, és mások az sms-beni vagy telefonos megkeresésekre.
- Az előző esetekhez hasonlóan számos kérdést felvet a honlapon keresztül fogadott álláspályázatra történő jelentkezés menete, melyet Adatvédelmi Szabályzatban kell rögzíteni. Minden esetben meg kell nevezni az adatkezelés jogalapját, célját, időtartamát, címzettjeit, és az érintetti jogokat is ismertetni kell.
- Adatvédelmi szempontból fontos körülmény, hogy kinek továbbítják a személyes adatokat. Ennek vonatkozásában naprakész nyilvántartással kell rendelkezni. A GDPR szerint például harmadik országba is továbbítható személyes adat, de ebben az esetben is fontos a megfelelőség biztosítása valamint erről az érintett tájékoztatása.
- Végül egy olyan lényeges összetevőt emelek ki, amelyet a megfelelésre való felkészülés során is szem előtt kell tartani: ellenőrizni kell, hogy az adatkezelő rendelkezik-e a törvényben megkívánt valamennyi nyilvántartással. Ezek a következők: adatkezelés nyilvántartása, adattovábbítási nyilvántartás, adatkezelési tevékenység megszüntetésére irányuló érintetti kérelmek nyilvántartása, incidens nyilvántartás. Az elszámoltathatóság elvének érvényre juttatásának céljából további nyilvántartások is rendelkezésre állnak: mint például az érintetti hatósági megkeresések nyilvántartása. Ezekben a nyilvántartásokban fel tudjuk tüntetni a megkereséseket valamint azokat az intézkedéseket is, amelyeket a feltárt problémák orvoslására tettek meg.

## INCIDENSKEZELÉS AZ UNIÓS SZABÁLYOZÁS KERETEIN BELÜL

Az adatvédelmi incidens[6] az adatvédelem egyik központi eleme, amelynek jelentését a GDPR az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvényhez (a továbbiakban Infotv.) képest kismértékben megváltoztatta. A Rendelet 4. cikk

[5] Az a természetes személy, aki adatok útján beazonosított vagy beazonosítható.

[6] Az adatvédelmi incidens a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi.

12. pont értelmében: *„Az adatvédelmi incidens a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi”.*

Már maga a definíció is jelzi, hogy rendkívül összetett feladatot jelent az adatvédelmi incidensek megelőzése. Sajnos a kiküszöbölésre tett óvintézkedések ellenére bekövetkezhetnek incidensek, ezért a GDPR nem csak a megelőzésre, de az adatvédelmi incidensek összetett kezelésére is nagy hangsúlyt fektet. A Rendelet 33. cikkének (5) bekezdése szerint az adatkezelő nyilvántartja az adatkezelési incidenseket, feltünteti az azokhoz kapcsolódó tényeket, annak hatásait és orvoslására történt intézkedéseket. E nyilvántartás segítségével a felügyeleti hatóság ellenőrizheti a GDPR-nak való megfelelőséget. Magyarországon a Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban Hatóság) tölti be a felügyeleti hatóság szerepét az adatvédelmi szabályok betartása felett.

A Rendelet egyértelművé teszi, hogy az adatkezelő[7] feladata az incidenskezelés, az adatfeldolgozó[8] ebben nem vesz részt, de adatvédelmi incidens bekövetkezése esetén haladéktalanul értesítenie kell az adatkezelőt.

A bekövetkezett incidens után az adatkezelőnek a Rendeletben meghatározott alábbi eljárásrendet kell követnie:

- Első lépésként meg kell határozni, hogy az incidens az érintett személyek jogára és szabadságára milyen hatással van.
- Második lépésként a bejelentést követően ne felejtsük el nyilvántartásba venni az incidenseket.
- Ezt követően az adatkezelő késedelem nélkül, de legfeljebb 72 órán belül bejelenti az incidenst a felügyeleti hatóságnak. Kivételt képez az az eset, amely során az adatvédelmi incidens vélhetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve.
- A Rendeletben meghatározott eljárásrend szerint meg kell határozni az incidens bekövetkezéséhez hozzájáruló potenciális forrásokat, hiányosságokat, felelősségeket, át kell vizsgálni a vállalkozás szabályozását, IT rendszerét, vagyis lépéseket kell tenni arra vonatkozólag, hogy a jövőben az adatvédelmi incidensek megelőzhetők lehessenek.

## ADATVÉDELMI INCIDENSEK SZANKCIONÁLÁSA

A GDPR az adatvédelmi kötelezettségeket, a mulasztás és jogsértés jogkövetkezményeit is jelentősen átalakította. Ez a felügyeleti eszköz nagyon rosszul érinti a vállalkozásokat. Az Infotv. szerint bírság kiszabása esetén a kiszabott bírság mértéke százezertől húszmillió forintig terjedhet. Az Infotv. szerint a hatóság figyelembe veszi az eset összes körülményét a bírság mértékének megállapításában, különös tekintettel figyel az érintettek számára, a jogsértés súlyára, valamint a jogsértés ismétlődő jellegét is mérlegeli. A hatósági gyakorlat a GDPR bevezetése előtt meglehetősen elnéző volt, az általános bírság súlyosabb esetben egymillió forint körül mozgott. Maximális bírság kiszabására csupán néhány esetben került sor.

A GDPR kötelező alkalmazása óta a szankciók köre jelentősen megváltozott. A Rendelet 58. cikke szerint a szankciók alkalmazása mind adatkezelőkre, mind adatfeldolgozókra egyaránt vonatkozik. A hatóság több módszert alkalmazhat, például figyelmeztet, elmarasztal

[7] Az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az érintett személyes adatait kezeli.

[8] Az adatkezelő tevékenységét segíti, önálló rendelkezési, döntési joga az adatok felett nincsen.

vagy megtilt, emellett természetesen lehetőség van bírság kiszabására is. Bírság kiszabása esetén fontos, hogy a bírság mértéke arányos legyen az incidens mértékével, valamint megfelelő visszatartó erővel kell bírnia. A bírság kiszabása azért is kockázatos a vállalkozások számára, mert súlyos esetben elérheti a húszmillió eurot vagy a vállalkozás előző pénzügyi éve teljes világpiaci forgalmának 4%-át.

Egy 2018. 05. 29-én benyújtott törvényjavaslat szerint az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény jogharmonizációs célú módosításáról szóló törvényjavaslat szerint az Infotv. a következő 75/A. §-sal egészülhet ki:

*„A Hatóság az általános adatvédelmi rendelet 83. cikk (2)-(6) bekezdésében foglalt hatásköreit az arányosság elvének figyelembevételével gyakorolja, különösen azzal, hogy a személyes adatok kezelésére vonatkozó – jogszabályban vagy az Európai Unió kötelező jogi aktusában meghatározott – előírások első alkalommal történő megsértése esetén a jogsértés orvoslása iránt – az általános adatvédelmi rendelet 58. cikkével összhangban – elsősorban az adatkezelő vagy adatfeldolgozó figyelmeztetésével intézkedik.”[4]*

Ez alapján kiemelendő tehát, hogy a Hatóság a számára rendelkezésre álló hatásköröket az arányosság elvének figyelembevételével gyakorolja, amely azzal valósul meg, hogy a Hatóság a jogsértés első alkalmával elsősorban – az eset összes körülményére, így a jogsértés súlyára, annak ismétlődő jellegére valamint az érintetti kör nagyságára is figyelemmel – az adatkezelő vagy adatfeldolgozó figyelmeztetésével intézkedik. Az arányosság elvének alkalmazása nagymértékben segítheti a kis-és középvállalkozásokat az őket megterhelő financiális szankciók elkerülése érdekében.

## KÖVETKEZTETÉSEK

Az adatvédelmi reformot követően az adatvédelmi jogszabályok 2018. Május 25 – től minden uniós országban azonosak. Ez közvetlen költségmegtakarítást és jogbiztonságot eredményez.

A szabályozás közvetlenül alkalmazandó minden olyan szervezetnél, amely személyes adatot kezel.

Az uniós rendelet hatályba lépése, az új irányelveknek való megfelelés jelentős átszervezési folyamatokat igényelt, új szervezeti változásokat követelt, új beruházások, infrastruktúra kialakítások váltak szükségessé.

A jogszabály a korábbinál szigorúbb elvárásokat támaszt az adatokat kezelőkkel, felhasználókkal szemben. Ezzel együtt sokkal nagyobb ellenőrzési lehetőséget kapnak a felhasználók saját személyes adataik és azok felhasználása felett, mint amivel korábban rendelkeztek.

A cikk segítséget nyújt a vállalkozásoknak adatvédelmi megfelelésük ellenőrzéséhez, rámutat arra is, hogyan kell eljárni egy előforduló incidens esetén, és milyen formában történhet az adatvédelmi incidensek szankcionálása.

## HIVATKOZÁSOK

[1] *Az uniós adatvédelmi reform: Milyen előnyökkel jár a vállalkozások számára Európában?* Európai Unió 2016, ISBN: 978-92-79-60207-8 http://ec.europa.eu/justice/data-protection/index_en.htm Letöltés ideje: 2017. 12. 21.

[2] https://ado.hu/rovatok/cegvilág/gdpr-mire-kell-figyelni Letöltés ideje: 2017. 12. 21.

[3] *Adatvédelem a gyakorlatban* HVG Kiadó Zrt. 2018, p. 22.

[4] „*Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvényjogharmonizációs célú módosításáról”*