Adatvédelem a gyakorlatban 2018

KIEGÉSZÍTÉS AZ ELMÚLT KÉT ÉV GYAKORLATI FEJLEMÉNYEIVEL

Mintegy két éve jelentettük meg az *Adatvédelem a gyakorlatban* című kiadványunkat, mely arra tett kísérletet, hogy érthetően, dióhéjban foglalja össze, és magyarázza el a személyes adatok védelmére vonatkozó megváltozott szabályanyagot, elsősorban a 2016/679. számú Általános Adatvédelmi Rendelet (GDPR) rendelkezéseit. Hazai és tagállami joggyakorlat, iránymutatások hiányában számos területen szempontrendszereket tudtunk csupán megfogalmazni. A kiadást követő két évben azonban mind a hazai, mind pedig a tagállami joggyakorlat jelentős mértékben alakult. Ezen túlmenően iránymutatásokkal segítette a tisztánlátást a European Data Protection Board (EDPB), illetve a European Data Protection Supervisor (EDPS). Ezen fejlemények eredményét az alábbiakban foglaljuk össze:

Az adatkezelő és az adatfeldolgozó elhatárolása[1]

Az elhatárolás kérdésében az EDPS iránymutatást tett közzé. Tekintettel arra, hogy a státusz meghatározása az adatkezelési kötelezettségek alapja, így ennek bemutatását részleteiben is megtesszük.

A GDPR definíciója szerint **adatkezelőnek** az minősül, aki az adatkezelés célját és eszközeit meghatározza. Az iránymutatás három csoportot különít el egymástól. Az első eset az, amikor az adatkezelői státuszt maga egy jogszabály hozza létre. Ezzel rokon eset az, amikor a jogalkotó feladatokat és hatáskört telepít valakire, és az így válik adatkezelővé. Az utolsó, lényegében a számunkra legfontosabb esetkör az, amikor a körülmények alapján válik valaki adatkezelővé. Az iránymutatás kiemeli, hogy az adatkezelői minőség feltétele a legfontosabb körülményekről való döntés: ő dönt arról, hogy milyen személyes adatokat, mennyi ideig kezelünk, kik válnak érintetté, kik férnek hozzá a személyes adatokhoz, valamint kiknek továbbítjuk a személyes adatokat. Adatkezelésre utalhat az is, ha ágazati szakmai szabályok hatálya alatt állunk (ügyvéd, orvos, könyvvizsgáló stb.). Nem zárja ki az adatkezelést az sem, ha az adatfeldolgozó bizonyos szintű önállósággal rendelkezik a hardver, szoftver, adatbiztonság területén feltéve, hogy az általános ellenőrzés, utasítás az adatkezelőnél marad. Az sem kizáró körülmény, ha a személyes adat nem is az adatkezelőnél, hanem az adatfeldolgozónál található, amennyiben az adatkezelés célját és eszközeit az adatkezelő határozza meg. Nem kizárt az sem, hogy egyszerre adatkezelői és adatfeldolgozói tevékenységet is végezzünk. Egy vállalat az ügyfelei, munkavállalói személyes adatai vonatkozásában adatkezelő. Amennyiben azonban egy másik vállalat kiszervezett bérszámfejtését is ellátja, abban az esetben e tekintetben adatfeldolgozóként jár el. Az ingatlanjog.hu ügyben pedig azt emelte ki a hatóság, hogy az adatkezelő ügyvéd abban az esetben, amikor a honlapot működtető vállalkozás számára kérdések megválaszolásában működött közre, adatfeldolgozói tevékenységet végzett.

Közös adatkezelésről akkor beszélünk, ha a személyes adatok kezelésének a célját és eszközeit többen, együttesen határozzák meg. Ilyen például a fejvadász és a megbízó cég viszonya, vagy a vállalkozás és a nevében eljáró megyei képviselők (mint vállalkozások). A lényeges körülmény az, hogy az adatkezelés célját kizárólag együttesen tudják elérni. Nem akadályozza a közös adatkezelés létrejöttét az a körülmény sem, hogy a felek az egyes cselekményeket nem közösen végzik, azaz beosztják egymás között. A közös adatkezelők felelőssége egyetemleges, így fokozottan egymásra vannak utalva. Ezért írja elő a GDPR megállapodás kötését (az adatfeldolgozói megállapodáshoz hasonlóan). Ennek tartalmi elemei között rendezni kell az adatbiztonság kérdését, azt, hogy az érintett a jogait hogyan tudja gyakorolni, ki lesz a kapcsolati pont, adatvédelmi incidens esetén milyen eljárásrendet követnek, illetve azt is szabályozni szükséges, hogy a felek mely esetekben, esetlegesen mely adatfeldolgozókkal köthetnek megállapodást.

Adatfeldolgozó az, aki a személyes adat kezelését más nevében, annak utasítása alapján végzi. A megkülönböztető jellege az, hogy míg az adatkezelő a saját célját valósítja meg, addig az adatfeldolgozó más céljait teljesíti be. Ilyen tevékenység lehet például informatikai rendszer kifejlesztése és üzemeltetése más számára úgy, hogy az adatkezelés célját, időtartamát, az érintetti kör és a címzetteket az ügyfél határozza meg. Fontos arra is rámutatni, hogy az adatkezelői státuszt bizonyos fokú önállóság nem hiúsítja meg. Az adatfeldolgozó akár tanácsot is adhat az adatkezelő részére, feltéve, hogy a végleges döntés meghozatala az adatkezelő kezében marad.

Jogalapok

A jogalapok közül a legfontosabban a szerződés teljesítése, illetve a jogos érdek. Előbbi vonatkozásában iránymutatást adott ki az EDPB[2]. Az iránymutatás leszögezi, hogy szerződés teljesítése, mint jogalap kizárólag azon személyes adatok kezeléséhez használható, melyek abszolút szükségesek a szerződés teljesítéséhez. Ilyen például egy webshopos rendelésnél a kiszállítási cím. Egyéb személyes adatok kezeléséhez (pl. érdeklődési körök) más jogalap fennállása szükséges.

[1] https://edps.europa.eu/data-protection/our-work/publications/guidelines/concepts-controller-processor-and-joint_en
[2] https://edpb.europa.eu/our-work-tools/our-documents/smernice/guidelines-22019-processing-personal-data-under-article-61b_en

Ilyen lehet a hozzájárulás vagy a jogos érdek. Egy webshopos rendeléssel összefüggésben például nem szükséges azt az adatkezelőnek tudnia, hogy milyen általános érdeklődési köre van a vevőnek. Amennyiben azonban valaki napi sajtószemle figyelését rendeli meg, annak szükséges eleme a preferenciák ismerete. Ezen megállapításokra támaszkodva kijelentette az iránymutatás, hogy a szolgáltatáshoz kapcsolódó csalásmegelőzés, ügyfélelégedettség stb. szintén nem szükségesek a szerződés teljesítéséhez, így meg kell jelölni azok önálló jogalapját.

Jogos érdek jogalap vonatkozásában a NAIH több alapvetést is lefektetett. Leszögezte, hogy a jogos érdek nem lehet kényelmi, gazdasági szempont. Kiemelte azt is, hogy az érdekmérlegelést érdekenként külön kell elvégezni, és mindegyik eredményéről szükséges az érintettet tájékoztatni. Különösképpen szigorúan mérlegelte a szükségesség-arányosság szempontrendszereit az elektronikus megfigyelőrendszerekkel összefüggő érdekmérlegelésekkel összefüggésben, és sok esetben arra a végkövetkeztetésre jutott, hogy annak indokoltsága nem támasztható alá (pl. önkormányzat területén kamera). A területtel külön bekezdésben foglalkozunk. A jogos érdek, mint jogalap egyre gyakrabban bukkan fel vállalkozásoknál, amelyek ügyfeleiknek kívánnak marketing üzenetet küldeni, valamint ez a jogalapja a személyes adatok átszállásának jogutódlás esetében is.

A közhatalmi jogosítvány gyakorlása, mint jogalap értelmezése hasonlóképpen jelentős fejlődésen ment keresztül. A Hatóság több döntésében, illetve a 2018. évre vonatkozó beszámolójában is kifejtette, hogy a közhatalmi szervek valamennyi jogviszonyukban közhatalmi jogosítvány gyakorlása (lényegében nem tudnak más jogalappal adatot kezelni), és nem jogos érdek alapján kezelik a személyes adatokat[3]. A jogalap alkalmazhatóságának keretei azonban a hatósági joggyakorlatban nem teljesen egyértelműek. A hatóság például a munkatársait közhatalmi jogosítvány gyakorlása jogalapon toborozza, a gyakornoki pályázatok adatkezelésének a jogalapja ugyanakkor szerződés teljesítése. A jogértelmezés a későbbi döntések tükrében fog kikristályosodni.

Az elektronikus megfigyelőrendszerek működésével összefüggésben EDPB-iránymutatás is elfogadásra került, mely meglehetősen szűk keretek között értelmezi az adatkezelési feltételeket. Az iránymutatás leszögezi, hogy a kamerahasználat nem alanyi jog, annak szükségességét és arányosságát érdekmérlegelés keretében alá kell támasztani, azaz végig kell venni és bemutatni az egyéb alternatívákat vagy azok hiányát. Az elvégzett érdekmérlegelést pedig időszakonként felül is kell vizsgálni. Az iránymutatás rövid adatkezelési határidőket tart szükségesnek és arányosnak, és szűken értelmezi a háztartási kivétel körét is. Ezen elvek érvényre juttatása a NAIH/2019/2076. számú döntésében nyomon követhető, amely döntésben a hatóság az önkormányzatnak azt rótta fel, hogy nem vizsgálta felül a megfigyelés szükségességét, valamint megkérdőjelezte, hogy önkormányzat esetében szükséges-e egyáltalán elektronikus megfigyelőrendszer használata. Az iránymutatás kitér a kapcsolódó cél területére is. Ez pedig azt takarja, hogy az eredetileg valamely céllal rögzített felvétel más célra felhasználható-e. Az iránymutatás itt sem biztosít tág mozgásteret az adatkezelőknek, mivel közvetlenül kapcsolódó cél esetében tartja megengedhetőnek a felvétel felhasználását (pl. jogérvényesítés céljából az ügyvédnek megküldik a vagyonvédelmi kamera felvételét). Ezen álláspontot a NAIH gyakorlatában már alkalmazza, s ennek értelmében szabott ki adatvédelmi bírságot a munkáltatóra, amiért a kamerafelvételt egy belső visszaélés felderítésére használta, holott a kamerát nem erre a célra telepítették. Aggályosnak tartotta továbbá a munkavállalók folyamatos megfigyelését is.[4]

Az ágazati jogszabályok módosítása

Az elmúlt két évben az ágazati jogszabályok közül számos módosításra került (pl. személy- és vagyonvédelem esetében a 2003. évi CXXXIII. törvény, a munka törvénykönyvéről szóló 2012. évi I. törvény). Ennek ellenére az ágazati jogszabályok GDPR-ral való összhangja továbbra sem biztosított. Egyrészt számos területen nem történt módosítás, más területeken pedig részleges törvénymódosítások történtek (pl. egészségügyi adatok kezelése, közszféra foglalkoztatási szabályai). Az adatkezelőknek tehát továbbra is kötelezettségük az ágazati jogszabályok GDPR-ba ütközésének vizsgálata, és adott esetben a GDPR szabályainak előnyben részesítése[5]. Ez ugyanakkor egy összetett jogi tudást feltételez az adatkezelők részéről, hiszen folyamatosan mérlegelniük szükséges egy adott szabály alkalmazhatóságát.

Érintetti jogok

Az érintetti jogokkal összefüggésben is több hazai, illetve tagállami döntés, iránymutatás született. A korábbiakban hivatkozott 3/2019. számú EDPB iránymutatás szerint a hozzáférési joga alapján ki kell adni az érintettnek a róla készült kamerafelvételt. A kiadással összefüggésben azonban gondosan kell eljárni, azaz a felvételen látható egyéb személyeket ki kell takarni. A hozzáférési jog terjedelme a vitája több munkajogi pernek is, melyekben a munkavállalók a róluk készült feljegyzések, értékelések kiadását is kérik. A munkáltató kötelezettsége vonatkozásában Németországban ellentétes döntések születtek. Az egyik ítélet szerint (Kölni Regionális Bíróság) az adatokat és nem az iratokat kell kiadni, a munkavállalóról készült feljegyzés, értékelés ugyanakkor nem tárgya a hozzáférési jognak. A NAIH több döntésében rámutatott arra, hogy az adatkezelőknek aktívan kell elősegíteniük az érintetti jogok gyakorlását. Amennyiben tehát az érintett az érintetti jogait nem helyesen gyakorolja, annak helyes módjáról is tájékoztatást kell nyújtani[6]. Végezetül véleményt tett közzé a NAIH a törlési kérelem megvalósítása vonatkozásában, melyben kiemelte a visszafordíthatatlanság és az elszámoltathatóság követelményeit[7].

[3] lsd.pl: NAIH/2019/2076
[4] NAIH/2019/2466
[5] NAIH/2018/5559
[6] NAIH/2019/1841
[7] NAIH/2019/2450

Adatvédelmi incidensek

Az adatvédelmi incidensek vonatkozásában is több hatósági döntés született. Ezek részben az incidensek súlyosságának minősítésével, illetve hozzá kapcsolódóan a bejelentési kötelezettség elmulasztásával[8], valamint az incidenskezelési eljárásrend hiányával foglalkoztak (ahol azt az adatkezelés jellege indokolja). Hangsúlyosan foglalkoznak a határozatok az incidenskezelési gyakorlat vizsgálatával[9], valamint a jogellenes adattovábbítással okozott incidensekkel[10].

Adatvédelmi hatásvizsgálat

A felügyeleti hatóság közzétette azon adatkezelések listáját, melyek esetében elvárja hatásvizsgálat lefolytatását[11]. Ezek közül a legfontosabbak a munkavállalók munkájának megfigyelése, például GPS gépjárműben történő elhelyezése vagy kamerás megfigyelés lopás vagy csalásmegelőzés céljából (16. pont). A hatóság honlapján egy hatásvizsgálati sablon is elérhető[12].

Adatvédelmi tisztviselő

Működik a hatóság online bejelentőrendszer, a hatóság kizárólag így fogadja el az adatvédelmi tisztviselők bejelentését. Amennyiben azonban az adatvédelmi tisztviselő személye változik vagy elírás történt a tisztviselő vagy az adatkezelő adataiban, abban az esetben a probléma elektronikusan nem orvosolható. A hatóságot levélben kell tájékoztatni, és ezzel egyidejűleg egy újabb bejelentést tenni a helyes adatokkal. Módosító funkció ugyanis jelenleg nem működik.

Munkaviszonnyal összefüggő adatkezelések

Az egyik legösszetettebb adatkezelési terület a foglalkoztatáshoz kapcsolódik. Az adatkezelőket megfelelésükben a munkavállalók ellenőrzésével összefüggésben szerencsére már döntések segítik[13]. Döntés született a munkavállalók munkavégzésének elektronikus megfigyelőrendszerrel történő megfigyeléséről[14], valamint az eszközhasználat ellenőrzéséről is[15]. A döntések kitérnek a magánhasználat engedélyezésének veszélyeire is, hiszen ebben az esetben közös adatkezelés jön létre, a munkáltató pedig a magánhasználathoz kapcsolódó személyes adatokat szándékán túl is archiválhatja. A döntések támpontokat adnak azt illetően is, hogy a munkahelyi ellenőrzéseket bemutató adatkezelési tájékoztató milyen elemeket tartalmazzon.

A foglalkoztatással összefüggő adatkezelések vonatkozásában rámutatunk arra, hogy a munka törvénykönyvéről szóló 2012. évi I. törvény adatkezelésre vonatkozó bekezdései alapvetően megváltoztak. A legfontosabb változások a bűnügyi személyes adat kezelhetőségére, a biometrikus adatok kezelésére, illetve a munkavállalói eszközhasználatra vonatkoznak. Utóbbi vonatkozásában a jogalkotó a törvényi vélelmet megfordította, jelenleg alaphelyzet az eszközök magánhasználatának tilalma, melyen a felek azonos akarattal változtathatnak.

Ügyféladatok kezelése

Az ügyféladatok kezelésének területe a természetes személy ügyfél, illetve az egyéni vállalkozó[16] ügyfél személyes adatainak a kezelése, hiszen a jogi személy adatainak a kezelése nem tartozik a GDPR szabályozási körébe. A területhez kapcsolódik továbbá a kapcsolattartó személyek személyes adatainak a kezelése is, mely vonatkozásában hatósági állásfoglalás áll rendelkezésre[17]. Ezzel összefüggésben ismételten rámutatunk az EDPB 2/2019. számú iránymutatására a szerződés teljesítésével összefüggő adatkezelésekről.

Az ügyféladatok kezelésével összefüggő hazai és tagállami, adatvédelmi bírságot is kiszabó döntések alapja az ügyféladatok korlátlan ideig történő kezelése, a HR és az ügyféladatbázis együttes kezelése, az aktív ügyféladatok, illetve az elévülési időtartam alatt „tárolt", esetleges igényérvényesítéshez szükséges adatok nem elkülönült kezelése.

Az adatvédelmi megfelelés ellenőrzése

A minták és a javaslatok egyszerűsített sablonokat tartalmaznak, melyek fő célja a szemléltetés. Nem mindegyik nyilvántartás kötelező a GDPR alapján (lásd adatvédelmi tisztviselő tevékenysége, megkeresések nyilvántartása, eltévedtlevél-nyilvántartás).

[8] NAIH/2019/0721
[9] NAIH/2019/2471
[10] NAIH/2019/2485, NAIH/2019/13
[11] https://www.naih.hu/files/GDPR_35_4_lista_HU_mod.pdf
[12] https://www.naih.hu/adatvedelmi-hatasvizsgalati-szoftver.html
[13] https://www.naih.hu/files/2019-12-19-kozlemeny-munkaltatoi-ellenorzesekkel-osszefuggo-adatkezelesekrol.pdf
[14] NAIH/2019/2076
[15] NAIH/2019/769, NAIH/2019/51/11
[16] https://www.naih.hu/files/NAIH-2018-5233-4-V.pdf
[17] https://www.naih.hu/files/NAIH_2018_3484_V_20180713.pdf

Ezek tekintetében az adatkezelő felelőssége azon döntés meghozatala, hogy a megfelelését milyen módon igazolja. Az egyes táblázatok terjedelmi okok miatt az adatkezeléseket összevontan mutatják be.

Az adatvédelmi megfelelés bizonyítása a GDPR 5. cikkében nevesített elszámoltathatóság elvének való megfelelés. Ezzel összefüggésben azonban a jogi környezet és a joggyakorlat megváltozott, így az adott részt az alábbi változtatásokkal javasolt követni:

Az adattovábbítási nyilvántartás megszűnt, így a továbbiakban ilyen kötelezettség az adatkezelőket nem terheli (24. oldal: eredeti minta az egyszerűen áttekinthető adattovábbítási nyilvántartáshoz). Hasonlóképpen nem szükséges adatkezelés megszűntetési kérelmekhez nyilvántartást vezetni. Az adattakarékosság elve alapján ugyanis nem javasolt a törölni kívánt személyes adatok egy részét újabb nyilvántartásban nevesíteni (kezelni) (24. oldal: Minta egyszerű adatkezelés-megszűntetési nyilvántartáshoz).

Az adatkezelési nyilvántartások között (26. oldal) a fentiek alapján nem kell szerepeltetni az adattovábbításokra vonatkozó nyilvántartási részt, illetve az adatkezelés megszűntetési kérelmekre vonatkozó részt (27. oldal).

Végezetül a GDPR 30. cikke szerinti belső nyilvántartások vonatkozásában mintaként a NAIH saját belső nyilvántartását is ajánljuk, mely közérdekű adatigénylés keretében kiadásra került, így hozzáférhető[18].

Információbiztonság

A GDPR 24., illetve 32. cikkei általános követelményrendszert fektetnek le. Ezek konkretizálása számos hazai és tagállami hatósági döntésben megvalósult. A NAIH több döntésében is az adatkezelő felelősségét állapította meg azon esetekben, amikor az adatfeldolgozó tevékenységéhez kapcsolódóan sérültek az integritás, bizalmi jelleg elvei[19]. A magyar hatóság tehát jellemzően az adatkezelő felelősségét állapítja meg (pl. T-Systems vs. BKK).

Az olasz hatóság azonban az Öt Csillag Mozgalommal kapcsolatos eljárásában kizárólag az adatfeldolgozó Rousseau Plattformot bírságolta meg, erre eddig kevés példa volt. A bírságot kiszabó határozat az egyszerű jelszókövetelményre, a sérülékenységi vizsgálat elégtelen voltára, a honlap nem biztonságos böngészési lehetőségére, a jelszavak egyszerű algoritmusokban való tárolására, illetve elégtelen anonimizálásra hivatkozott. Hasonló aggályokra hivatkozva szabott ki bírságot a felügyeleti hatóság a Demokratikus Koalícióra is[20].

Végezetül jellemző jogsértés ebben a körben az adatfeldolgozási megállapodás megkötésének elmaradása vagy csupán sablonos adatfeldolgozási szerződés kötése. Az adatfeldolgozási megállapodás léte ugyanakkor kulcskérdés, annak tartalmára vonatkozó garanciális elemeket a GDPR 28. cikke tartalmazza.

Ezek közül a legfontosabbak az adatfeldolgozás kereteinek nevesítése (kinek a nevében pontosan milyen tevékenység, melyek az érintett személyes adatok), az utasításhoz kötöttség vállalása, rendelkezés aladatfeldolgozó bevonhatóságáról, adatfeldolgozói közreműködési kötelezettség az érintetti jogok gyakorlásával, incidenskezeléssel, illetve hatósági vizsgálatokkal összefüggésben.

[18] https://kimittud.atlatszo.hu/request/a_hatosag_adatkezelesi_tevekenys
[19] NAIH/2018/776/H, NAIH/2018/356/3/H
[20] NAIH/2019/2668