FORUM

2020. február

II. évfolyam, 2. szám

GDPR Őrszem

Elektronikus változáskövető szaklap

iratmintákkal és tanácsadói szolgáltatással

GDPR: kevés a felkészült szervezet, egyre több a bírság

Már több mint 140 millió forint GDPR-bírságot szabtak ki a Magyarországon működő cégekre, a legtöbb szervezet késik a GDPR megfeleléshez szükséges IT-fejlesztések befejezésével, amivel további bírságokat kockáztatnak – hívja fel a figyelmet az EY.

A közlemény szerint esetenként átlagosan 2,5 millió forint értékben, eddig összesen 58 alkalommal szabott ki bírságot hazai cégekre a Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) 2018 májusa óta az általános adatvédelmi rendelet megsértéséért. Magyarország ezzel az egyik leggyakrabban fellépő ország Európa szerte Spanyolország, Románia, Németország és Bulgária mellett.

Európában az eddigi legnagyobb, több mint 66 milliárd forintos bírságot a British Airways könyvelhette el, de szintén több tízmilliárdot kellett fizetnie a GDPR megsértése miatt a nemzetközi szállodaláncnak, a Marriott International-nek.

Zala Mihály, az EY információbiztonsággal foglalkozó vezetője szerint a számokból egyértelműen látszik, hogy véget ért a türelmi időszak. Míg 2018-ban mindössze 151 millió forint bírságot szabtak ki az európai adatvédelmi hatóságok, tavaly már a 130 milliárd forintot is meghaladta ez az összeg – mutatott rá a közleményben.

Leggyakrabban a személyes adatok kezelésére vonatkozó elvet sértik meg a vállalatok, amiért az elmúlt mintegy másfél évben már 58 alkalommal büntetett a NAIH. Európában ezért 79 esetben szabtak ki büntetést a felettes szervek. Szintén gyakran vétenek a cégek az adatkezelés jogszerűsége (68 eset) és az adatkezelés biztonsága ellen (48 eset).

A rendelet bevezetésekor a legtöbb cég megtette az alapvető intézkedéseket a megfelelés érdekében. Adatkezelési nyilvántartást vezetett be, elvégezte a szükséges hatásvizsgálatokat vagy oktatta például a dolgozóit. Ezt követően azonban sokan fellélegeztek, és továbbra is késnek a szükséges IT-fejlesztésekkel – emelte ki Zala Mihály.

> Míg 2018-ban mindössze 151 millió forint bírságot szabtak ki az európai adatvédelmi hatóságok, tavaly már a 130 milliárd forintot is meghaladta ez az összeg.

A szakember szerint ez azért okoz jelentős kockázatot, mert a kiberbűnözők folyamatosan keresik azokat az elavult szoftvereket, amin keresztül könnyen és gyorsan lophatnak tömegesen személyes adatot. Egy sikeres támadás pedig, mint ahogy arra már hazai példát is lehetett látni, nagyon gyorsan vezethet több tíz, vagy akár százmillió forintos bírsághoz is.

Forrás: mti.hu

Foglalkoztatással kapcsolatos adatkezelések egyes kérdései

IV. rész

Mottó: *„Igazságot hirdetni, vagy hasznos dolgokat javasolni az embereknek, biztos módja annak, hogy üldözzenek minket."*
(Voltaire[1])

Cikksorozatunk előző részében megkezdtük annak vizsgálatát, hogy a foglalkoztatással összefüggő adatkezelések során a GDPR 6. cikkelyében meghatározott jogalapok közül miért nem alkalmazható általános jelleggel a 6. cikk a.) pontjában megjelölt „hozzájárulás". Ezentúl érdemes megjelölni, hogy vannak olyan esetek, amikor a hozzájárulás – kifejezetten szűk körben – mégis alkalmazható lehet a foglalkoztatási jogviszony létrehozása előtt és a jogviszony alatt is, bizonyos élethelyzetekben.

Jelen cikkünkben kizárólag a hozzájárulás azon esetét vizsgáljuk, amikor az álláspályázatra jelentkező személy esetében alkalmazhatóvá válik az érintett hozzájárulása mint lehetséges jogalap. Ezen jogalap alkalmazása során azonban nagyon óvatosan kell eljárnunk, mivel amennyiben nem állnak fent a jogalap alkalmazásának feltételei, akkor az adatkezelés jogellenes lesz. Tovább nehezíti az amúgy sem egyszerű helyzetünket az a tény, hogy sok esetben nagyon nehéz még egy jogász számára is beazonosítani, hogy az adatkezelő által bemutatott jogviszony a valóságban is azt fedi-e le, amelyet az adatkezelő számunkra megjelölt. Kezeljük minden esetben kellő fenntartással azokat a helyzeteket, amelyek álláspontunk szerint a felek közötti jogviszonyrendszerbe inkább munkaviszony-jellegűek. Tekintve, hogy a WP 249. számú Vélemény kiemeli annak jelentőségét, hogy a 29. számú munkacsoport a „munkavállaló" kifejezést nem kívánja szűken értelmezni, így nem kizárólag a munkaviszonyban álló személyekre rendeli el az abban foglaltakat. Ennek következtében a WP 249. számú Véleményben foglaltakat bizonyos körülmények fennállása esetén nem csak azon alkalmazottak esetén kell figyelembe venni, akik munkaszerződéssel rendelkeznek, és akik a mindenkor hatályos munkaügyi jogszabályok értelmében munkavállalónak minősülnek. Tehát adójogi és munkajogi szempontú és vonatkozású vizsgálataink során sokkal nagyobb körültekintéssel kell megközelítenünk a felek jogviszonyát, de az adatkezelés szempontjából segítségünkre siet a WP 249. számú Vélemény, amely kifejezetten helyesen vonja a szabályozási kör alá azokat az üzleti és piaci modelleket, amelyek éppen az információs technológia elmúlt évtizedeiben zajló robbanásszerű fejlődése során egyre inkább elterjedtté váltak. A WP 249. számú Vélemény ezen kitétele szerint különösen ide sorolhatók azok a személyek is, akik a felek téves vagy megtévesztő szándéka alapján egyébként önálló vállalkozók vagy megbízottak, azonban a felek közötti jogviszony tartalmi jellemzői alapján a valóságban munkaviszonyban állnak. *„Ez a vélemény le kíván fedni minden olyan helyzetet, ahol munkaviszony áll fenn, függetlenül attól, hogy ez a viszony munkaszerződésen alapul-e."*[2]

Ezen kérdéskör mélyebb taglalása jelen cikk keretein túlmutat, de összességében annyit mindenképpen érdemes leszögezni, hogy óvatosan kell eljárni akkor, amikor egy adott munkafolyamat tekintetében feltétel nélkül elfogadjuk az adatkezelő azon állítását, hogy a felek között nem munkaviszony, hanem vállalkozási vagy megbízási jogviszony áll fent. A jogviszonyok tartalmi jellemzői alapján az Adóhatóság bizonyos feltételek fennállása esetén egyébként is munkaviszonnyá minősítheti ezen jogviszonyokat.

[1] https://idezetabc.hu/idezetek/voltaire/igazsagot-hirdetni-vagy-hasznos-dolgokat
[2] https://www.naih.hu/files/wp249_hu_munkahelyi_adatkezelesek.pdf

A cikk írója szerint tényleg mérlegelni kell a WP 249. számú Vélemény fentiekben idézett kiterjesztő szabályozását, és ennek megfelelően kell beazonosítani az adatkezelés megfelelő jogalapját.

Visszatérve a hozzájárulás kérdéskörére, adatkezelési szempontból a WP 249. számú Vélemény a következőket rögzíti:

„Fontos kimondani, hogy a munkavállalók a munkáltató és a munkavállalók közötti függőségi viszonyból eredően ritkán vannak abban a helyzetben, hogy szabadon megadják, megtagadják vagy visszavonják a hozzájárulásukat. Kivételes helyzetektől eltekintve a munkáltatóknak más, a hozzájárulástól eltérő jogalapra kell támaszkodniuk, mint például az adatok munkáltató jogos érdekei céljából történő kezelése…”[3]

Tehát jogosan merül fel a kedves olvasóban a kérdés, hogy akkor mely esetekben alkalmazható jogszerűen a hozzájárulás mint lehetséges jogalap. A cikk írójának álláspontja szerint jogszerűen alkalmazható a hozzájárulás mint lehetséges jogalap azokban az esetekben, amikor az állásra jelentkező személy önéletrajzát a pályázat befogadója kezeli, és ezen hozzájárulás alapján akár a rendszerében a tájékoztatásban megjelölt határidőig tárolja. Ennek azért van nagy jelentősége, mert az állásra jelentkező személy megküldi az önéletrajzát az adatkezelő vagy bizonyos esetben az adatfeldolgozó részére. Az adatkezelő és az adatfeldolgozó által kialakított eljárásrend és szabályzati háttér akkor felel meg a GDPR rendelkezéseinek és NAIH elvárásainak, ha már az adatkezelés megkezdése előtt az érintett birtokában van az az információ, amely alapján döntési helyzetbe kerülhet a személyes adatait illetően. Vagyis az érintettnek pontos információt kell kapnia az adatkezelés minden részletéről ahhoz, hogy ezen ismeretek birtokában megfelelő döntési pozícióba kerüljön. Az érintettnek alapvető joga, hogy saját maga döntsön abban a kérdésben, hogy az ismertetett feltételekkel megadja a személyes adatait vagy sem. Tudnia kell pontosan, hogy mely személyes adatok kezeléséhez járul hozzá, vagy a megadott hozzájárulását, hogyan vonhatja vissza. Az cikk írójának álláspontja szerint az álláspályázatok benyújtását megelőzően is kiemelt jelentősége van annak, hogy a jelentkező megfelelő formában és módon tájékoztatásra kerüljön az adatai kezelése tekintetében. Adatvédelmi Tisztviselőként kiemelt figyelmet kell fordítanunk arra, hogy az adott adatkezelő belső rendszerének ismeretében minden részfolyamat során megfelelő határidőben kiadásra kerüljenek a szükséges adatkezelési tájékoztatások. Egy elutasított pályázó vagy egy haragos volt munkavállaló kellemetlen pillanatokat okozhat az adatkezelő számára, amennyiben a kötelező tájékoztatások hiányában panasszal fordul a hatóság felé.

A cikk írójának álláspontja szerint jogszerűen alkalmazható a hozzájárulás mint lehetséges jogalap azokban az esetekben, amikor az állásra jelentkező személy önéletrajzát a pályázat befogadója kezeli, és ezen hozzájárulás alapján akár a rendszerében a tájékoztatásban megjelölt határidőig tárolja.

Nem lehet elégszer hangsúlyozni annak jelentőségét, hogy Adatvédelmi Tisztviselőként minden egyes adatkezelő és adatfeldolgozó tekintetében részletesen meg kell vizsgálni a felvétel és elbocsátás során alkalmazott folyamatokat. Adatvédelemmel foglalkozó szakemberként minden esetben az oktatások megszervezésével és lebonyolításával egyidejűleg kötelező feladat, hogy a foglalkoztató szektorális elhelyezkedésének figyelembevétele mellett folyamatosan nyomon kísérjük az eljárási folyamatok esetleges változását. Gyakran szembesülni fogunk azzal, hogy a HR vezetők részéről érzékelhető egy igen aktív ellenállás ebben a körben, bár ez egyre inkább nem számottevő. Kevés HR vezető szívébe lopjuk be magunkat azzal, ha felszólítjuk őket a nem megfelelő jogalap nélkül kezelt, tárolt önéletrajzok – jegyzőkönyv kíséretében – történő azonnali megsemmisítésére. Szerencsére, ebben is látható egy igen erőteljes pozitív változás, de van még hova fejlődni.

A GDPR (39) preambulumbekezdése szerint: *„A személyes adatok kezelésének jogszerűnek és tisztességesnek kell lennie. A természetes személyek számára átláthatónak kell lennie, hogy a rájuk vonatkozó személyes adataikat hogyan gyűjtik, használják fel, azokba hogy tekintenek bele vagy milyen egyéb módon kezelik, valamint azzal összefüggésben, hogy a személyes adatokat milyen mértékben kezelik vagy fogják kezelni. Az átláthatóság elve megköveteli, hogy a személyes adatok kezelésével összefüggő tájékoz-*

[3] https://www.naih.hu/files/wp249_hu_munkahelyi_adatkezelesek.pdf

tatás, illetve kommunikáció könnyen hozzáférhető és közérthető legyen, valamint, hogy azt világosan és egyszerű nyelvezettel fogalmazzák meg. Ez az elv vonatkozik különösen az érintetteknek az adatkezelő kilétéről és az adatkezelés céljáról való tájékoztatására, valamint az azt célzó további tájékoztatásra, hogy biztosított legyen az érintett személyes adatainak tisztességes és átlátható kezelése, továbbá arra a tájékoztatásra, hogy az érintetteknek jogukban áll megerősítést és tájékoztatást kapni a róluk kezelt adatokról. A természetes személyt a személyes adatok kezelésével összefüggő kockázatokról, szabályokról, garanciákról és jogokról tájékoztatni kell, valamint arról, hogy hogyan gyakorolhatja az adatkezelés kapcsán megillető jogokat.

> Nem lehet elégszer hangsúlyozni annak jelentőségét, hogy Adatvédelmi Tisztviselőként minden egyes adatkezelő és adatfeldolgozó tekintetében részletesen meg kell vizsgálni a felvétel és elbocsátás során alkalmazott folyamatokat

A személyes adatkezelés konkrét céljainak mindenekelőtt explicit módon megfogalmazottaknak és jogszerűeknek, továbbá már a személyes adatok gyűjtésének időpontjában meghatározottaknak kell lenniük. A személyes adatoknak a kezelésük céljára alkalmasaknak és relevánsaknak kell lenniük, az adatok körét pedig a célhoz szükséges minimumra kell korlátozni. Ehhez pedig biztosítani kell különösen azt, hogy a személyes adatok tárolása a lehető legrövidebb időtartamra korlátozódjon. Személyes adatok csak abban az esetben kezelhetők, ha az adatkezelés célját egyéb eszközzel észszerű módon nem lehetséges elérni. Annak biztosítása érdekében, hogy a személyes adatok tárolása a szükséges időtartamra korlátozódjon, az adatkezelő törlési vagy rendszeres felülvizsgálati határidőket állapít meg. A pontatlan személyes adatok helyesbítése vagy törlése érdekében minden észszerű lépést meg kell tenni. A személyes adatokat olyan módon kell kezelni, amely biztosítja azok megfelelő szintű biztonságát és bizalmas kezelését, többek között annak érdekében, hogy megakadályozza a személyes adatokhoz és a személyes adatok kezeléséhez használt eszközökhöz való jogosulatlan hozzáférést, illetve azok jogosulatlan felhasználását."

Tehát abban az esetben, ha álláspályázatot közlünk, alapvető elvárás, hogy a jelentkező számára közérthető formában tartalmazza legalább a fentieknek megfelelő lényegi információkat, de a tájékoztató konkrét tartalmáról később még részletesebben és behatóbban fogunk értekezni. Ezen tájékoztató közlésével szemben, valamint maga a tájékoztatás megtörténtének igazolása tekintetében alapvető elvárás, hogy az elszámoltathatóság szuperelve alapján minden bizonyítható legyen. Fontos, hogy bizonyítani tudjuk, hogy az érintett, vagyis a jelentkező a döntése meghozatala előtt megismerhette a tájékoztató tartalmát. Így amennyiben a foglalkoztató rendelkezik honlappal, akkor érdemes a tájékoztatót ott is elhelyezni, és a feladott álláshirdetésben megjelölni a linket. Amennyiben a foglalkoztató nem rendelkezik honlappal, akkor az is jó megoldás lehet, hogy a jelentkező számára feladatott hirdetésben vagy megjelölik a szükséges adatokat, vagy közölnek egy e-mail címet, amelyre elküldve egy automatikus válasz e-mailben írásban megküldik a pályázó részére a tájékoztatást tartalmazó válaszlevelet. Utóbbi esetben fontos a hirdetésben rögzíteni, hogy a jelentkező mindenképpen olyan e-mail címet használjon, amely nem tartalmaz személyes adatot, tehát, amely alapján nem lesz a jelentkező azonosítható.

Adatvédelmi Tisztviselőként részletes és tételes írásos kimutatást kell kérni arról, hogy a foglalkoztató a pályázó felkutatása során mely fejvadász cégekkel, munkaerő-közvetítővel, munkaerő-kölcsönzővel, diákszövetkezettel, nyugdíjas szövetkezettel stb. áll kapcsolatban. Nagyon sokszor nem is olyan egyszerű azt sem eldönteni, hogy közös adatkezelésről van szó, vagy éppen adatfeldolgozói státuszt tölt be a munkaerőt ajánló vagy kiközvetítő cég, hiszen maga az adatkezelés, így egyben a közös „munka" határozza meg, hogy adatfeldolgozói megállapodást kötnek a felek vagy közös adatkezelői megállapodást. Ezentúl minden esetben szükséges az is, hogy alaposan megismerjük a felek közötti viszonyt, a munkamegosztást, és átnézzük a már megkötött szerződéseket, vagy a jövőben megkötendő szerződésekben különös hangsúlyt fektessünk arra, hogyan kerülnek szabályozásra a felek jogai és kötelezettségei, a felelősségi kérdések, hiszen a GDPR szabályai itt is lényeges előírásokat tartalmaznak. Ezen kérdéskörre a cikksorozat további részeiben részletesebben kitérünk.

Szerző: Dr. Dvorán Gabriella LL.M.
adatvédelmi- és adatbiztonsági szakjogász
munkajogi szakjogász
adójogi szakjogász

WP29 állásfoglalás: Hogyan vonatkoznak az érintett jogainak gyakorlására irányadó szabályok az adathordozhatóságra?

Az érintett részére milyen előzetes információt kell megadni?

Annak érdekében, hogy az adatkezelők megfeleljenek az adathordozhatósághoz való új jognak, tájékoztatniuk kell az érintetteket az adathordozhatósághoz való új jog meglétéről. Ha az érintett személyes adatokat közvetlenül az érintettől gyűjtik be, erre „a személyes adatok megszerzésének időpontjában" kell sort keríteni. Ha a személyes adatokat nem közvetlenül az érintettől szerzik meg, az adatkezelőnek meg kell adnia a 13. cikk (2) bekezdésének b) pontjában és 14. cikk (2) bekezdésének c) pontjában említett információt.

„Ha a személyes adatokat nem az érintettől szerezték meg", a 14. cikk (3) bekezdésének megfelelően az információt a személyes adatok megszerzésétől számított észszerű határidőn, de legkésőbb egy hónapon belül, az érintettel való első kapcsolatfelvétel alkalmával vagy harmadik személyekkel való közléskor meg kell adni[1].

A kért információ megadásakor az adatkezelőnek biztosítania kell, hogy elkülönítik az adathordozhatósághoz való jogot más jogoktól. A 29. cikk szerinti munkacsoport tehát különösen azt ajánlja, hogy az adatkezelők fejtsék ki egyértelműen, hogy az érintett milyen típusú adatokat kaphat meg a hozzáférési joga, és milyeneket az adathordozhatósághoz való joga keretében.

Ezenfelül a munkacsoport azt ajánlja, hogy az adatkezelők mindig tüntessenek fel információt az adathordozhatósághoz való jogról, mielőtt az érintett megszüntetné valamelyik fiókját. Ez lehetővé teszi a felhasználók számára, hogy számba vegyék személyes adataikat, és könnyen továbbítsák őket saját készülékükre vagy egy másik szolgáltatóhoz, mielőtt a szerződés megszűnne.

Végül, a „címzett" adatkezelők számára bevált gyakorlatként a 29. cikk szerinti munkacsoport azt ajánlja, hogy az érintetteket lássák el teljes körű információval azon személyes adatok jellegéről, amelyek a szolgáltatás teljesítése szempontjából relevánsak. Amellett, hogy megalapozza a tisztességes adatkezelést, ez lehetővé teszi a felhasználók számára, hogy korlátozzák harmadik személyek kockázatait, és a személyes adatok szükségtelen megduplázódását, akkor is, ha más érintettet nem fognak a műveletbe bevonni.

Hogyan tudja az adatkezelő azonosítani az érintettet a kérelme megválaszolása előtt?

Az általános adatvédelmi rendeletben nincsenek előíró jellegű követelmények az érintett hitelesítésére. Az általános adatvédelmi rendelet 12. cikkének (2) bekezdése mindazonáltal kimondja, hogy az adatkezelő az érintett jogai (az adathordozhatósághoz való jogot is ideértve) gyakorlására irányuló kérelmének a teljesítését nem tagadhatja meg, kivéve, ha olyan cél érdekében kezeli a személyes adatot, amelyhez az érintett azonosítása nem szükséges, és bizonyítja, hogy az érintettet nem áll módjában azonosítani. Ilyen helyzetben ugyanakkor a 11. cikk (2) bekezdése szerint az érintett kiegészítő információt adhat meg, amely lehetővé teszi az azonosítását. Ezenfelül, a 12. cikk (6) bekezdése úgy rendelkezik, hogy ha az adatkezelőnek megalapozott kétségei vannak az érintett kilétével kapcsolatban, további, az érintett személyazonosságának megerősítéséhez szükséges információk nyújtását kérheti. Ha az érintett kiegészítő információt ad, amely lehetővé teszi azonosítását, az adatkezelő nem tagadhatja meg a kérelem teljesítését. Ha az online gyűjtött információk és adatok álnevekhez vagy egyedi azonosítókhoz kötődnek, az adatkezelők megfelelő eljárásokat alkalmazhatnak, amelyek lehetővé teszik az egyének számára az adathordozhatósági kérelem benyújtását és a rájuk vonatkozó adatok megszerzését. Akárhogy is, az adatkezelőknek le kell futtatniuk egy hitelesítési eljárást annak érdekében, hogy határozottan meggyőződjenek a személyes adatait kérelmező, vagy általánosabban, az általános adatvédelmi rendelet szerinti jogait gyakorló érintett személyazonosságáról.

Ezek az eljárások gyakran már rendelkezésre állnak. Az érintetteket az

[1] A 12. cikk előírja, hogy az adatkezelő „minden egyes tájékoztatást tömör, átlátható, érthető és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazva nyújtsa, különösen a gyermekeknek címzett bármely információ esetében."

adatkezelő már gyakran a szerződéskötés vagy az adatkezeléshez való hozzájárulás beszerzése előtt hitelesíti. Ennek következtében az adatkezeléssel érintett egyén nyilvántartására használt személyes adatokat az érintett hordozhatósági célú hitelesítésének bizonyítékaként is fel lehet használni[2].

Noha ezekben az esetekben az érintettek előzetes azonosításához esetleg be kell kérni személyazonosságuk bizonyítékát, az ilyen ellenőrzés lehet, hogy nem releváns az adat és az érintett egyén közötti kapcsolat értékelése szempontjából, mivel e kapcsolat nem függ össze a hivatalos vagy jogi személyazonossággal. Lényegében az adatkezelő azon lehetősége, hogy kiegészítő információt kérjen be adott személy személyazonosságának értékelése céljából, nem vezethet túlzó kérésekhez és olyan személyes adatok begyűjtéséhez, amelyek nem relevánsak vagy szükségesek az egyén és a kért személyes adat közötti kapcsolat megerősítése szempontjából.

Sok esetben ilyen hitelesítési eljárások már hatályban vannak. Például felhasználóneveket és jelszavakat gyakran használnak arra, hogy lehetővé tegyék az egyén hozzáférését az e-mail- fiókjában, közösségi hálózati fiókjaiban vagy számos más szolgáltatáshoz használt fiókjaiban található adataihoz; e fiókok némelyikét az egyének teljes nevük és személyazonosságuk felfedése nélkül veszik igénybe.

Ha az érintett által kért adatok mérete miatt problematikus az internetes adattovábbítás, ahelyett, hogy esetlegesen hosszabb, legfeljebb három hónapos határidőt venne igénybe a kérelemnek való megfelelésre[3], az adatkezelőnek esetleg meg kell fontolnia az ilyen adat rendelkezésre bocsátásának alternatív eszközeit, például az online közvetítést, illetve a CD-re, DVD-re vagy más fizikai eszközre való lementést, vagy annak lehetővé tételét, hogy a személyes adatot közvetlenül egy másik adatkezelőhöz továbbítsák (az általános adatvédelmi rendelet 20. cikkének (2) bekezdése szerint, ha műszakilag megvalósítható).

Mi az adathordozhatósági kérelem megválaszolásának határideje?

A 12. cikk (3) bekezdése előírja, hogy „az adatkezelő indokolatlan késedelem nélkül, de mindenféleképpen a kérelem beérkezésétől számított egy hónapon belül tájékoztatja az érintettet a [...] hozott intézkedésekről". Ez az egyhónapos időszak kiterjeszthető legfeljebb három hónapra az összetett esetekben, ha az érintettet tájékoztatták e késedelem okairól az eredeti kérelem beérkezésétől számított egy hónapon belül.

Az információs társadalommal összefüggő szolgáltatást működtető adatkezelők valószínűleg jobban felszereltek ahhoz, hogy a kérelmeket nagyon rövid időn belül teljesítsék. A felhasználói elvárásoknak való megfelelés érdekében bevált gyakorlat olyan időkeret meghatározása, amelyen belül az adathordozhatósági kérelem szokásosan megválaszolható, továbbá ennek közlése az érintettekkel.

Azok az adatkezelők, akik elutasítják az adathordozhatósági kérelmet, a 12. cikk (4) bekezdése szerint a kérelem beérkezésétől számított egy hónapon belül tájékoztatják az érintettet „az intézkedés elmaradásának okairól, valamint arról, hogy az érintett panaszt nyújthat be valamely felügyeleti hatóságnál, és élhet bírósági jogorvoslati jogával."

Az adatkezelőknek be kell tartaniuk a megadott határidőn belüli válaszadásra vonatkozó kötelezettséget, akkor is, ha ez elutasítást jelent. Más szóval, az adatkezelőknek nyilatkozniuk kell, ha adathordozhatósági kérelemmel fordulnak hozzájuk.

Milyen esetekben utasítható el az adathordozhatósági kérelem vagy állapítható meg díj?

A 12. cikk tiltja, hogy az adatkezelő díjat állapítson meg a személyes adatok rendelkezésre bocsátásáért, kivéve, ha az adatkezelő bizonyítani tudja, hogy a kérelem egyértelműen megalapozatlan vagy „– különösen ismétlődő jellege miatt –" túlzó. Azon információs társadalommal összefüggő szolgáltatások számára, amelyek személyes adatok automatizált kezelésére szakosodtak, az automatizált rendszerek, például a felhasználói program interfészek (API-k)[4] működtetése megkönnyítheti az érintettel való kapcsolattartást, ezáltal csökkennek az ismétlődő kérelmek jelentette esetleges akadályok. Ezért nagyon kevés olyan eset van, amikor az adatkezelő meg tudja indokolni a kért információ átadásának megtagadását, még többszörös adathordozhatósági kérelem esetén is.

Ezenfelül, az adathordozhatósági kérelmek megválaszolására létrehozott eljárások teljes költségét figyelmen kívül kell hagyni a kérelem túlzó mértékének megállapításánál. Az általános adatvédelmi rendelet 12. cikke ugyanis az egyetlen érintett által benyújtott kérelmekre összpontosít, nem az adatkezelő által kézhez vett

[2] Ha például az adatkezelés felhasználói fiókhoz köthető, a megfelelő felhasználói név és jelszó megadása elegendő lehet az érintett azonosításához.

[3] A 12. cikk (3) bekezdésében: „Az adatkezelő [...] tájékoztatja az érintettet a [...] kérelem nyomán hozott intézkedésekről."

[4] A felhasználói program interfész (API) alkalmazások és webszolgáltatások interfészét jelenti, amelyet az adatkezelők bocsátottak rendelkezésre, hogy más rendszerek vagy alkalmazások kapcsolódhassanak az ő rendszereikhez, és együttműködhessenek velük.

kérelmek teljes számára. Ennek eredményeként a rendszer működtetésének teljes költsége egyfelől nem hárítható át az érintettre, másfelől nem használható a hordozhatósági kérelmek megválaszolása elutasításának indokolására.

Melyek az adatszolgáltatás teljesítésének adatkezelőtől elvárt eszközei?

Az általános adatvédelmi rendelet 20. cikkének (1) bekezdése szerint az érintettek jogosultak arra, hogy az adatokat egy másik adatkezelőnek továbbítsák anélkül, hogy ezt akadályozná az az adatkezelő, amelynek a személyes adatokat a rendelkezésére bocsátották.

Ez az akadályoztatás leírható olyan jogi, műszaki vagy pénzügyi akadályként, amelyet az adatkezelő állított, hogy fékezze vagy lassítsa az érintett vagy más adatkezelő általi hozzáférést, továbbítást vagy további felhasználást. Ilyen akadályok lehetnek például a következők: az adatszolgáltatásért kért díj, az interoperabilitás hiánya vagy az adott adatformátumhoz, API-hez, vagy az előírt formátumhoz való hozzáférés hiánya, túlzott késedelem vagy a teljes adatállomány lekérdezésének összetettsége, az adatállomány szándékos összezavarása, egyedi és indokolatlan vagy túlzó ágazati szabványosítás, vagy akkreditációs követelmények.[5]

A 20. cikk (2) bekezdése azt a kötelezettséget is megállapítja az adatkezelő számára, hogy a hordozható adatot közvetlenül más adatkezelőnek továbbítsa, „ha az technikailag megvalósítható".

Az adatkezelők közötti, az érintett rendelkezése szerinti adattovábbítás technikai megvalósíthatóságát esetről esetre kell értékelni. A (68) preambulumbekezdés ezen felül pontosítja a „technikai megvalósíthatóság" korlátait, miszerint az „nem teremthet olyan kötelezettséget az adatkezelők számára, hogy egymással műszakilag kompatibilis adatkezelő rendszereket vezessenek be vagy tartsanak fenn".

Az adatkezelőktől elvárt, hogy a személyes adatokat interoperábilis formátumban továbbítsák, noha ez nem kötelezi arra a többi adatkezelőt, hogy e formátumokat támogassák. Az adatkezelők közötti közvetlen adattovábbításra tehát akkor lehet sort keríteni, ha a két rendszer közötti kommunikáció lehetséges biztonságosan[6], és ha a címzett rendszer műszakilag képes a bejövő adatok fogadására. Ha műszaki akadályok gátolják a közvetlen adattovábbítást, az adatkezelőnek magyarázatot kell adnia ezen akadályokra az érintetteknek, mivel döntése egyébként hasonló lenne hatásában az érintett kérelmével kapcsolatos intézkedés megtagadásához (12. cikk (4) bekezdés).

Műszaki szinten az adatkezelőknek két különböző és egymást kiegészítő utat kell feltárnia és értékelnie, hogy a hordozható adatot az érintett vagy a másik adatkezelő rendelkezésére bocsássa:

- a hordozható adatok teljes állományának (vagy a teljes adatállomány részei több kivonatának) közvetlen továbbítása;
- automatizált eszköz, amely lehetővé teszi a megfelelő adatok kivonatolását.

A második módszert az adatkezelők akkor részesíthetik előnyben, ha összetett és nagy adatállományról van szó, mivel e módszer lehetővé teszi az adatállomány bármely, az érintett számára kérelmével összefüggésben releváns részének kivonatolását, segíthet a kockázat minimalizálásában, és valószínűleg lehetővé teszi adatszinkronizációs mechanizmusok[7] alkalmazását (pl. az adatkezelők közötti rendszeres kommunikáció keretében). Jobb módszere lehet a megfelelés garantálásának az „új" adatkezelő vonatkozásában, és bevált gyakorlatnak minősülhet a magánéletvédelmi kockázatok csökkentésében az eredeti adatkezelőnél.

A megfelelő hordozható adatok átadásának e két különböző és lehetőség szerint egymást kiegészítő módja megvalósítható az adatok számos eszközzel történő rendelkezésre bocsátásával, például biztonságos üzenetváltással, SFTP-szerverrel, biztonságos WebAPI-vel vagy webportállal. Az érintettek számára lehetővé kell tenni, hogy egy személyesadat-tárat, személyes információt kezelő rendszert[8] vagy más típusú megbízható harmadik felet vegyenek igénybe a személyes adatok megőrzésére és tárolására, és hogy engedélyt adjanak az adatkezelőknek a személyes adatokhoz való hozzáférésre és azok kezelésére, igény szerint.

Forrás: WP29 Guidelines

[5] Egyes akadályok jogszerűek lehetnek, mint amelyek mások 20. cikk (4) bekezdésében említett jogaihoz és szabadságához kapcsolódnak, vagy amelyek az adatkezelő saját rendszereinek biztonságával függnek össze. Az adatkezelő felelőssége megindokolni, hogy az ilyen akadályok miért jogszerűek és miért nem minősülnek a 20. cikk (1) bekezdésének értelmében vett akadályoztatásnak.

[6] Hitelesített kommunikációval a szükséges adattitkosítás mellett.

[7] A szinkronizációs mechanizmus segíthet az általános adatvédelmi rendelet 5. cikke szerinti általános kötelezettségek teljesítésében, amely cikk szerint „a személyes adtok[nak...] pontosnak és szükség esetén naprakésznek kell lenniük".

[8] A személyes információt kezelő rendszerekről lásd például az európai adatvédelmi biztos 9/2016. számú véleményét, amely elérhető itt: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2016/16-10-20_PIMS_opinion_EN.pdf

Óvodai, iskolai **adatkezelés**

Az lenne a kérdésem, hogy a gyermekek óvodába és iskolába beiratkozásakor milyen személyes dokumentumokat lehet elkérni, illetve lefénymásolni? Adatkezelés hozzájárulás nyilatkozat mintájuk van-e általános iskolák és óvodák részére?

Véleményünk szerint az igazolványok másolása/szkennelése nem jogszerű, túlmutat a célhoz kötöttség, a szükségesség-arányosság (adatminimalizálás) elvén, nem szükségesek, jogszabály ezek rögzítését nem írja el, sőt, jogszabály csak bemutatásról rendelkezik:

„Az óvodai beiratkozáskor be kell mutatni a gyermek nevére kiállított személyazonosságot igazoló hatósági igazolványokat, továbbá a szülő személyazonosságát igazoló hatósági igazolványokat és lakcímet igazoló hatósági igazolványát." (20/2012. (VIII. 31.) EMMI rendelet 20. § (3) bek.)

Tehát a jogszabály csak a bemutatást követeli meg, nem a másolást/szkennelést.

„Az általános iskola első évfolyamára történő beiratkozáskor be kell mutatni a gyermek nevére kiállított személyazonosságot igazoló hatósági igazolványokat." (20/2012. (VIII. 31.) EMMI rendelet 22. § (4) bek.)

Mivel bemutatás a kötelező, ezért a másolás/szkennelés nem alkalmazható.

A konkrét, jogszerű célhoz kell készíteni hozzájáruló nyilatkozatot, így általános minta nincsen.

Jegyzőkönyv

(Panaszkezelési Szabályzat _ sz. melléklete)

Panasz azonosítója:			
Panasz felvételének dátuma:			
Panasz felvételének helye:			
Panasz felvevője (Munkatárs neve), elérhetősége:			
Panasz előterjesztésének módja:	Írásbeli	Szóbeli	
Szóbeli bejelentés esetén:	Személyesen szóban	Képviselő útján szóban	Személyesen telefonon
Panaszos neve:			
Panaszos kapcsolattartójának neve:			
Panaszos telefonszáma:			
Panaszos képviselőjének neve, levelezési címe, telefonszáma:			
A telefonhívás időpontja (ha telefonon történt a panasz bejelentése):			
Szóbeli panasz előterjesztésének időpontja (ha nem telefonon történt):			
Panaszolt szolgáltatás:			
Tények, csatolt dokumentumok (ha vannak):			
Panasz oka:			
Maga a panasz:			
Panaszos igénye:			
Üzemeltető nyilatkozata a panasszal kapcsolatos álláspontjáról, amennyiben a panasz azonnali kivizsgálása lehetséges/Panasz orvoslásának módja, ideje:			
Panasszal kapcsolatos döntés várható időpontja (ha nem azonnali):			

(Szükség esetén pótlappal bővíthető!)

Kmf.

Üzemeltető részéről aláírás

Panaszos/Panaszos képviselőjének aláírása

Az **iratmintát** szerkeszthető formában letöltheti weboldalunkról is!

Tipikus adatkezelések

Egyszeri információcsere

Az egyszeri információcserén, vagy egyszeri információ kérésen és -adáson azt az adatkezelést érthetjük, amikor egy érintett egy egyszeri kérdését az adatkezelő megválaszolja, és ezzel gyakorlatilag az adatkezelés célja meg is szűnik, mert nem következik belőle semmi.

Példa lehet erre egy érintett által küldött e-mail, amelyben az érintett az iránt érdeklődik, hogy az adatkezelő irodája mikor van nyitva. Nem időpontot foglalt, pusztán csak a nyitva tartás érdekelte. Vagy éppen telefonon arról érdeklődött az érintett, hogy van-e kapacitása az adatkezelőnek valamilyen feladat ellátására, például egy konyhabútor legyártására, azonban az adatkezelőnek nincsen kapacitása, válasza nemleges, tehát a felek lezárják az ügyet, a témát. Lehet egy véletlenül érkezett e-mail, vagy telefonhívás is.

Egyszeri kérdés, válasz, további lépések nem következnek belőle, joghatás nincsen. Ahogyan ez látható, az adatkezelés megvalósult, mert a célja megvalósult a válasszal, ebből aztán az következik, hogy cél nélkül adatokat kezelni nem lehet, tehát egy ilyen információ kérő e-mailt, a válasszal együtt törölni kell(ene). Sőt, a híváslistából is törölni lenne szükséges az egyszeri kérdező telefonszámát. Számos adatkezelő ez utóbbira legyint, de ha arra gondolunk, hogy a mai modern világban a telefon híváslistáját a személygépjármű szoftvere egyszerűen átveszi, letárolja, akkor már duplikálódott az adat, teljesen feleslegesen, sőt, lehet, hogy az autószerviz számítógépe a szervizelés alkalmával ezt biztonsági mentésként lemásolja, valahol, egy felhőben. Abban az esetben, ha az adatkezelő tud más jogalapot, például megalapozott jogos érdeket felmutatni az adatok további kezelése vonatkozásában, akkor természetesen az alapján lehet az adatokat kezelni.

Előfordulhat, hogy az adatkezelő jogszabály alapján köteles rögzített vonalú telefont üzemeltetni, ilyenkor természetesen a vonatkozó jogszabály rendelkezéseit kell betartani és az abban meghatározott időtartamban fogja tárolni a hangfelvételt. Az is előfordulhat, hogy az adatkezelő keresi meg az érintettet, stb. Érdemesnek mutatkozik az egyes célokat, módokat felderíteni és meghatározni a tájékoztatókat.

Levelezés

Tipikus az, hogy az adatkezelő és az érintett egymással e-mailt (levelet) váltanak, amelynek alapja tipikusan valamilyen jogviszony, vagy éppen annak előkészítése. A korábbiak alapján tehát lehet egy ilyen adatkezelés alapja a GDPR 6. cikk 1. szakasz b) pontja, tehát az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél, vagy az a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges. De lehet önkéntes hozzájárulás, sőt lehet jogi kötelezettség teljesítése, vagy más jogalap is. (Kapcsolattartók adatainak kezelése kapcsán a jogos érdek lesz a jogalap.) Maradva a megállapodáson alapuló adatkezelésnél, az adatkezelő jogszerűen fogja kezelni a levelezés során megszerzett személyes adatokat. Már csak azt kell eldönteni, hogy mennyi ideig kezeli az adatokat jogszerűen. Nagyon gyakran az adatkezelés időtartama a jogviszony megszűnését követő elévülésig (tipikusan 5 évig) tart tekintettel arra, hogy elképzelhető az, hogy valamilyen jogérvényesítés merül fel akár az adatkezelő, akár az érintett oldaláról. Gyártó cégek esetében, például egy autóipari beszállító esetében felmerülhet a következő: az adatkezelő olyan szabványok, előírások alapján dolgozik, amelyek kötelezővé teszik adatok visszakereshetőségét akár 10-15 évre is, például fejlesztési vagy éppen gyártási dokumentációval kapcsolatban. Ha ehhez kapcsolódik levelezés, akkor a levelezést is tudni kell ennyi ideig megjeleníthetően tárolni, kezelni. Nem ritkán az ilyen gyártók külön számítástechnikai eszközt is letárolnak, hogy megjeleníthető legyen a segítségével a 15 évvel azelőtti fejlesztési/gyártási dokumentáció, nehogy szoftveres kompatibilitási problémák miatt (lásd például operációs rendszerek elmúlt 20-25 éves fejlődését) ne lehessen azt megjeleníteni, megvizsgálni. Ezért egy adatkezelőnek figyelembe kell vennie a rá vonatkozó jogi kötelezettségeket is az adatok tárolása, kezelése kapcsán.

Már most látszik, hogy az e-mail fiókban különböző célú és különböző időtartamban tárolt adatok lapulnak, amelyeket fel kell fedezni és törölni kell. Ehhez megoldás az utasítások kiadása, végrehajtása és ellenőrzése lehet.

GDPR Őrszem | II. évfolyam 2. szám | 2020. február | Kiadja a Forum Média Kiadó Kft. | 1139 Budapest, Váci út 91. | Tel.: +36 1 273 2090 • Fax: +36 1 468 2917 | Felelős kiadó: Rok Podgornik | Szerkesztő: Hoppál Előd | Hirdetések felvétele: +36 1 273 2090, +36 1 273 2099 | Fax: +36 1 467 2917 | E-mail: ugyfelszolgalat@forum-media.hu | Internet: www.forum-media.hu | Tördelés: B-TEX 2000 Bt. | Képek: Depositphotos, Pixabay | MTI Sajtófelhasználó | Előfizethető a kiadónál.