ADATVÉDELMI ÖRÖKMOZGÓ MEGOLDHATATLAN FELADVÁNYOK A GDPR-BÓL

SZERZŐ: DR. DÓSA IMRE, JOGÁSZ, JOGI INFORMATIKUS, 2004. ÓTA FOGLALKOZIK INTENZÍVEN ADATVÉDELEMMEL

Az általános európai adatvédelmi rendelet megalkotói alapjogi hevülettel láttak neki munkájuknak.
A jogszabály szigorát általános fogalmakkal igyekeztek széleskörűvé tenni.

Egy lépésben kívánták letudni a rendkívül egyszerű - mondhatjuk úgy is, hogy a hétköznapi jogalanyok számára ingerküszöb alatti - és az egyes emberek számára áttekinthetetlenül komplex adatkezelések szabályozását. Az eredmény első látásra tetszetős volt. Sőt, az adatkezelések nagy dögkeselyűivel szemben kiszabott látványos bírságok látszólag megerősítették ezt. A cél érthető és méltánylást érdemlő volt. Sem új technikai vívmányokkal, sem bagatellizáló kivételekkel ne lehessen kibújni a szabályok alól. A GDPR, mint eszköz azonban ott tévesztett célt, hogy az “egy méret mindenkire jó” elve nem mérkőzött meg az ókori Rómában kidolgozott “omnis definitio in iure civili periculosa est” (minden definíció a polgári jogban veszélyes) gondolatával.

A GDPR-ból hiányzik az elvárhatóság elve. Ezen kívül felállítja azt a vélelmet, hogy az átlagos érintett képes megérteni az adatkezelés részleteit, összetettségét, majd a megértés alapján akár le is mond azon előnyökről, jogviszonyokról, melyek érdekében adatait kezelik az adatkezelők. Nagyon ritkán van alkalmunk ilyen tudatossággal találkozni. Sőt, sokan az adatvédelmi tudatosságot csodabogár tulajdonságnak tekintik. Ez persze nem véletlen. A GDPR (az alapjául szolgáló irányelv modelljét követve) nagyon egyszerű adatkezeléseket tekint mintának. Erre fűzte fel mind az adatkezelői kötelezettségek, mind az érintetteket megillető jogok rendszerét. Közben a bennünket övező világ - benne az adatkezelések - komplexitása annyit fejlődött, hogy a GDPR modellje minden adatkezelőt jogsértővé tett. Ez azért rontja jelentősen az adatvédelem hatékonyságát, mert többségünk vonakodva indul eleve vesztes csatába.

Kárhoztatható az adatkezelő, ha formális megfelelésre (vagy még arra sem) törekszik olyan adatkezeléseknél, melyek esetén bármikor megbüntethetik? Nehezen. Ezért érdemes áttekinteni néhány olyan példát, melyet mindenki használ, és amely esetén az adatvédelmi hatóságok a homokba dugják a fejüket, az "amit nem látok, azt nem bánom" elve alapján. Pedig fontos lenne, hogy hatóság is kimondja a GDPR alkalmazhatatlanságát. Szembesüljön a GDPR követelmények egyes esetekben mutatkozó gyakorlati képtelenségével, és azzal, hogy ez nem az adatkezelők, hanem a szabályozási logika hibája.

Spam szűrő

Mindenki használja, mert nélküle leállna az email forgalom. Működéséről az átlag érdeklődő annyit szokott tudni, hogy nagy nemzetközi szolgáltatóknál érdemes előfizetni, akik hatalmas levél forgalmat elemezve állapítják meg, hogy melyik levél spam.A szűrés szabályait titkolják, azért hogy a kéretlen levelek küldői ne tudják megkerülni azokat. Annyit azért lehet tudni, hogy számtalan esetben a szűrés nem csak egy adott tárgyú levélre vagy egy adott feladóra terjed ki, hanem akár a feladóval azonos levelező szerveren lévőkre is. Ha egy spam szűrő kiszűr egy levelet, akkor törli, de erről semmilyen értesítést nem küld. Hiszen ha küldene, a hibaüzenetek lavinája indulna el a hamisított feladók miatt.

A rövid leírás sejteti, miért nem lehet találkozni a spam szűrésre vonatkozó dokumentációkkal. Személyes adatok kezelése megvalósul? Igen. Születik automatizált döntés a levél célba juttatásáról? Igen. Érintheti jelentősen a címzett jogait, ha például álláspályázatot nyújtott be egy céghez? Igen. Biztosítható az érintett bármilyen adatvédelmi joga? Például a tájékoztatáshoz (beleértve az alkalmazott logikáról tájékoztatáshoz való jogot is), a tiltakozáshoz, a törléshez, a helyesbítéshez, az emberi felülvizsgálathoz való jogot? Rendre nem. Teljesíthető a harmadik országba történő adattovábbítással, adatfeldolgozói szerződéssel kapcsolatos adatkezelői kötelezettség? Ezek sem. Ennek okai könnyen beláthatók. Például a korlátozott tárolhatóság, majd a törlés nem alkalmazható, mert a szűrés hatékonyságát veszélyeztetné. A szűrő program üzemeltetője pedig saját céljára (a minták finomítására, gazdagítására) használja fel a vizsgált adatokat, tehát nem köt adatfeldolgozói megállapodást. Sérti a GDPR-t a spam szűrés? Minden elemében. Mondhatjuk, hogy felhagyunk a tömeges, jogellenes adatkezeléssel? Nem. Hogyan lépi át az adatvédelem a feloldhatatlan problémát? Létezéséről sem vesz tudomást. Nem lenne tisztességesebb kimondani, hogy világunknak vannak adatkezelési vakfoltjai, melyek szabályozására a GDPR alkalmatlan?

Szerintem igen. Sokan fellélegeznének. Persze csak azok, akik komolyan veszik az adatvédelmet, nem törődnek bele abba, hogy a GDPR politikai-hatalmi fenyegetés eszközévé legyen lezülleszthető.

Céges mobil

A GDPR 2. cikk (2) c) pontja kiveszi a jogszabály hatálya alól az adatkezelést, ha azt természetes személyek kizárólag személyes vagy otthoni tevékenységük keretében végzik. Az Európai Adatvédelmi Testület szerint ezt a kivételt nem szabad kiterjesztően értelmezni. Ezt az az értelmezést követi az adatvédelmi hatóságok gyakorlata is. Ezért a céges mobiltelefon nem vonható az idézett kivétel alá. Ha belegondolunk, vajon Európa-szerte mennyi adatkezelést érint ez a szemlélet? A korszerű készülékek híváslistái, sms tárai több száz hívás, üzenet adatait is megőrizhetik. Vessünk egy pillantást ennek adatvédelmi megfelelésére:

Abban egységes az adatvédelmi szakma, hogy a telefonszám önmagában azonosíthatja az előfizetőt, használót, ezért a telefonszám magában is személyes adat. Felhívtam egy céges mobilszámot. A híváslistába bekerült a hívószámom, a hívás ideje, időtartama. Utólag törölhető, de nem hallottam olyan készülékről, amelyen kikapcsolható lenne.

Mi ezen adatkezelés célja? Leginkább az, hogy visszahívhassanak. Ha pusztán ez a cél, a cégek, hatóságok hoztak olyan szabályt, hogy a visszahívással nem érintett hívásokat a munkavállaló haladéktalanul törölje? Aligha. Pedig a célját veszített adatkezelés jogellenes. Sérti a korlátozott tárolhatóság elvét. Tömeges, alapelvi sérelem történik. Ezért már vastagon fog a hatóság ceruzája a büntető csekken. Pedig még csak az elemzés elején tartunk. Az érintett az adatkezelésről semmilyen tájékoztatást nem kap. Ezért adatvédelmi jogait sem tudja gyakorolni, ami további alapelvi sérelemre vezet. Ha a telefon használója - valljuk be, többségünk ilyen - nem tudja memghekkelni a telefont, akkor a készülék a címjegyzéket a telefon operációs rendszerének megfelelő - tipikusan USA-ban letelepült - szolgáltató felhő alkalmazásában tárolja. Erre az adatfeldolgozásra akkor sem köthetnénk adatfeldolgozói megállapodást, ha szeretnénk. A munkáltatók mobil device management rendszerei sem támogatják a telefonok ilyen irányú adatvédelmi megfelelését. Abba is ijesztő belegondolni, egy telefon elvesztése esetén miként értesíthetők az adatvédelmi incidens kárvallottjai.

A mobiltelefon többi szolgáltatása, az üzenetek több platformos kezelése, az alkalmazások engedélyezhető adat összekapcsolásai, a helyadatok, fényképek kezelése mind-mind megoldhatatlan adatvédelmi rémálom. Ennek ellenére használjuk. Azok sem tolják el maguktól arcukon enyhe undorral, akik adatvédelmi tudatosságot élnek meg - például azért, mert adatvédelmi hatóságnál dolgoznak.

Van kiút?

Remélem a példák jól szemléltették, hogy a való élet, a három dimenziós világ adatkezeléseinek hétköznapjai milyen konokul ellenállnak a GDPR két dimenziós, papírra nyomtatott világának - és a sematikusan ezt követő egysíkú hatósági gyakorlatoknak. Ha ennek tudatalatti hátterét keressük, könnyű eljutni az “ingerküszöb alatti adatkezelés” fogalmához. Melyet nem az elméleti megfelelés, hanem a tömeges, háborítatlan használat tesz társadalmilag elfogadottá. A valóság azt mutatja, ez fontosabb, mint az elméleti adatvédelmi tisztaság. Ezt a jelenséget más jogágak már tudják kezelni. A korábban említett elvárhatósági mérce bevezetésével az adatvédelmi megfelelés iránti igény a valóban fontos irányokra, területekre fókuszálhatna.