Az adatvédelem európai útvesztőjében

Mobilszolgáltatójuktól, bankjuktól, civil szervezettől sokan kaptak májusban értesítést arról, hogy az elkövetkezőkben hogyan kezelik majd személyes adataikat. Május 25-én lépett életbe ugyanis az Európai Parlament és az Európai Unió Tanácsának (EU) 2016/679. számú rendelete, az európai általános adatvédelmi rendelet (General Data Protection Regulation – GDPR).

Bár magát a rendeletet több mint két éve, 2016. április 27-én fogadták el, jó hazai szokás szerint legtöbben a huszonnegyedik órában, azaz májusban kezdtek el utánanézni annak, mit is jelent ez, és mivel jár az alkalmazása a közintézményekre és vállalkozásokra nézve, illetve mit is jelent ez a magánszemélyek számára. A rendelet szövegének alapos áttanulmányozása után azonban félő, hogy az amúgy jó kezdeményezés belefullad majd a bürokráciába. Sokan a bírságoktól tartanak, hiszen azok kiszabható összege az adatforgalmi rendelkezés egyes szabályainak megsértése esetén elérheti a tíz- vagy a húszmillió eurót, illetve a vállalkozások az előző pénzügyi év teljes éves piaci forgalmának legfeljebb 2 vagy 4 százalékát kitevő összeggel sújthatók. Minden esetben a magasabb összeget kell kiszabni bírságként.

Kötelező lépések

A GDPR előírásait 2018. május 25-től kell alkalmazni valamennyi európai uniós tagállamban. A 37. cikkely értelmében „Az adatkezelő és az adatfeldolgozó adatvédelmi tisztviselőt jelöl ki minden olyan esetben, ha:

a) az adatkezelést közhatalmi szervek vagy egyéb, közfeladatot ellátó szervek végzik, kivéve az igazságszolgáltatási feladatkörükben eljáró bíróságokat;
b) az adatkezelő vagy az adatfeldolgozó fő tevékenységei olyan adatkezelési műveleteket foglalnak magukban, amelyek jellegüknél, hatókörüknél és/vagy céljaiknál fogva az érintettek rendszeres és nagymértékű megfigyelését teszik szükségessé;
c) az adatkezelő vagy az adatfeldolgozó fő tevékenységei a személyes adatok 9. cikkely szerinti különleges kategóriáinak és a 10. cikkelyben említett, büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó adatoknak nagy számban való kezelését foglalják magukban.”

Az adatvédelmi tisztviselő (Data Protection Officer) kijelölése nem kötelező a 250 embernél kevesebbet foglalkoztató magánvállalkozások számára, a Romániában létrehozott felügyeleti szerv, a Személyes Adatok Feldolgozását Felügyelő Országos Hatóság (Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal) mégis ajánlja, mivel ez biztosíthatja a GDPR betartását. Az adatvédelmi felelős elérhetőségét az intézmények, vállalatok honlapján is közzé kell tenni. Ha nincs mód külön adatvédelmi tisztviselő kijelölésére, szolgáltatási szerződést kell kötni egy külsőssel, esetleg a feladattal olyan alkalmazottat kell megbízni, akinek munkaköre nem

összeférhetetlen ezzel a tisztséggel. Bár nincs pontos lista arról, kiket nem nevezhetnek ki adatvédelmi tisztviselővé, összeférhetetlenség általában a vezetők esetében áll fenn, mivel ők befolyásolhatják az adatfeldolgozást vagy adatkezelést.

Szintén kötelező lépés – a 250 főnél kevesebbet foglalkoztató magánvállalkozások számára is – egy úgynevezett leltár készítése, melyből kiderül, ki foglalkozik a személyes adatok kezelésével, milyen személyes adatokat kezel, milyen céllal, kinek továbbít személyes adatokat, meddig őrzi meg a személyes adatokat (mind papíron, mind elektronikus nyilvántartásban), és milyen intézkedéseket hozott a személyes adatok védelméért.

Hogyan gyűjtik, mire használják adatainkat?

Valószínűleg mindenki hallott a Cambridge Analytica-botrányról, ha máshonnan nem, a Facebook tájékoztatásából: ő vagy ismerősei adatai eljutottak-e vagy sem a céghez. A vállalatot azzal vádolták, hogy jogosulatlanul kezelte legalább 87 millió Facebook-felhasználó személyes adatait, melyeket egy látszólag ártalmatlan személyiségteszt-applikáció segítségével gyűjtött be róluk. Az információkat politikai tanácsadásra használta fel, a többi közt Donald Trump választási kampányában.

Mindannyian tapasztalhattuk, hogy akár a mobiltelefonos alkalmazások, akár a Facebookon használt különféle játékok, tesztek kérik, hogy hozzáférjenek például telefonszámunkhoz, sms-einkhez, ismerőseink listájához. Arra is volt példa, hogy egy-egy ilyen jóváhagyás után a kedveléseink között megjelent például politikai párt vagy akár előadó oldala, holott bizton tudtuk: nem „lájkoltuk" az illető oldalát. Az internethasználók előtt az sem ismeretlen jelenség, hogy ha rákeresnek valamire (hitelfelvétel, telefon-, autó- stb. vásárlás), akkor a közösségi oldalon nagyszámú olyan reklám kerül eléjük, amely összefügg a kereséssel.

Adatokat gyűjtenek például a hűségkártyákkal is, hiszen azok használatával látszik, hol és milyen gyakorisággal, milyen termékeket vásárolunk.

Számtalan módja van tehát az adatgyűjtésnek, s ha ezeket az adatokat biztonságosan kezelik, használják, probléma sem származik belőle. Ha azonban az adatok kiszivárognak, ellopják őket, jelentős anyagi és erkölcsi kárunk is származhat belőle. Hiszen ha valaki hozzáférhet az e-mail-postaládánkhoz, a nevünkben azt írhat, akinek és amit akar, vagy ha ellopják bankszámlánk adatait, elköthetik a pénzünket.

Mi számít személyes adatnak?

Arról, hogy mi számít személyes adatnak, a rendelet első fejezetének 4. cikkelyében olvashatunk, ugyanott tisztáznak más alapfogalmakat is.

Személyes adat tehát a rendelet szerint az „azonosított vagy azonosítható természetes személyre (»érintett«) vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható".

A meghatározás első látásra elég általános, kicsit szűkít rajta a 87. cikkely, mely szerint „a tagállamok részletesebben meghatározhatják a nemzeti azonosító számok vagy egyéb általános jellegű azonosító jelek

kezelésének konkrét feltételeit. Ebben az esetben a nemzeti azonosító számok, illetve az egyéb általános jellegű azonosító jelek felhasználására kizárólag az érintett jogainak és szabadságainak e rendelet szerinti megfelelő garanciái mellett kerülhet sor".

Romániában a 2001-ben elfogadott és azóta többször módosított 677. számú adatvédelmi törvény szabályozza a személyes adatok védelmét és feldolgozását. A GDPR-ről szóló egyik tanfolyamon elhangzott: az uniós jog bizonyos esetekben felülírja a nemzeti szabályozást, az adatvédelem pedig ilyen terület. A romániai törvényhozóknak módjukban áll tehát pontosítani az egyes területek szabályozását, de csak a GDPR-rel összhangban.

A személyes adatoknak vannak úgynevezett különleges kategóriáik, melyek kezelését néhány kivételtől eltekintve tiltja a rendelet. A II. fejezet 9. cikkelyének első bekezdése így szól: „A faji vagy etnikai származásra, politikai véleményre, vallási, világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a természetes személyek egyedi azonosítását célzó genetikai és biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok kezelése tilos."

A kivételek között szerepel, ha „az érintett kifejezett hozzájárulását adta az említett személyes adatok egy vagy több konkrét célból való kezeléséhez, kivéve, ha az uniós vagy tagállami jog úgy rendelkezik, hogy az (1) bekezdésben említett tilalom nem oldható fel az érintett hozzájárulásával", továbbá ha „az adatkezelés az adatkezelőnek vagy az érintettnek a foglalkoztatást, valamint a szociális biztonságot és szociális védelmet szabályozó jogi előírásokból fakadó kötelezettségei teljesítése és konkrét jogai gyakorlása érdekében szükséges, ha az érintett alapvető jogait és érdekeit védő megfelelő garanciákról is rendelkező uniós vagy tagállami jog, illetve a tagállami jog szerinti kollektív szerződés ezt lehetővé teszi". Kivétel a szabály alól az is, ha az az adatkezelésre valaki létfontosságú érdekeinek védelmében van szükség, ez olyan adatokra vonatkozik, amelyeket az érintett kifejezetten nyilvánosságra hozott, az adatkezelésre egészségügyi vagy népegészségügyi (például járványmegelőzési) célokból van szükség. A tagállamok további feltételeket – köztük korlátozásokat – tarthatnak hatályban, illetve vezethetnek be a genetikai adatok, a biometrikus adatok és az egészségügyi adatok kezelésére vonatkozóan.

Szintén kivételt jelent a szabály alól, ha „az adatkezelés valamely politikai, világnézeti, vallási vagy szakszervezeti célú alapítvány, egyesület vagy bármely más nonprofit szervezet megfelelő garanciák mellett végzett jogszerű tevékenysége keretében történik, azzal a feltétellel, hogy az adatkezelés kizárólag az ilyen szerv jelenlegi vagy volt tagjaira vagy olyan személyekre vonatkozik, akik a szervezettel rendszeres kapcsolatban állnak a szervezet céljaihoz kapcsolódóan, és hogy a személyes adatokat az érintettek hozzájárulása nélkül nem teszik hozzáférhetővé a szervezeten kívüli személyek számára".

Ha valaki gyermekeknek kínál az információs társadalommal összefüggő szolgáltatásokat, az ő adataik kezelése akkor számít jogszerűnek, ha a gyermek legalább a 16. évét betöltötte; a 16 évesnél fiatalabbak adatainak kezeléséhez a szülői felügyeletet gyakorló beleegyezése szükséges. Ennek ellenőrzésére az adatkezelőnek „ésszerű erőfeszítéseket" kell tennie. A tagállamoknak itt is van némi mozgásterük, törvényben megszabhatnak alacsonyabb életkort, de legtöbb három évvel szállíthatják le a korhatárt (13 évre).

És a címlistám?

Felvetődhet kérdés, mi a helyzet például a saját címjegyzékünkkel, telefonszám- vagy e-mail-cím-listánkkal, hiszen az abban szereplő adatok is személyes adatnak minősülnek. A rendelet 18. cikkelye azonban leszögezi: „ez a rendelet nem alkalmazandó a személyes adatoknak a természetes személy által kizárólag személyes vagy otthoni tevékenység keretében végzett kezelésére, amely így semmilyen szakmai vagy üzleti tevékenységgel nem hozható összefüggésbe. Személyes vagy otthoni tevékenységnek minősül a levelezés, a címtárolás, valamint az említett személyes és otthoni tevékenységek keretében végzett, közösségi hálózatokon való kapcsolattartás és online tevékenységek. E rendeletet kell alkalmazni azonban azokra az adatkezelőkre és adatfeldolgozókra, akik a személyes adatok ilyen személyes vagy otthoni tevékenység keretében végzett kezeléséhez az eszközöket biztosítják."

Ha tévedésből kapunk e-mailt, annak tartalmát tilos nyilvánosságra hozni, a küldő felet viszont figyelmeztethetjük. Ha pedig olyasvalakitől kapunk – például reklám célú – elektronikus levelet, akinek nem adtuk meg e-mail-címünket, jogunk van rákérdezni, hogyan és kitől kerültek személyes adataink az illető birtokába, és erről tájékoztatást is kell kapnunk.

Mihez van jogunk személyes adatainkkal kapcsolatban?

A rendelet az érintettek jogait a III. fejezetben szabályozza. Ha személyes adatainkat tőlünk gyűjtötték, az adatgyűjtéskor az adatkezelőnek tudatnia kell velük az alább felsoroltakat:

„*a)* az adatkezelőnek és – ha van ilyen – az adatkezelő képviselőjének a kiléte és elérhetőségei;
b) az adatvédelmi tisztviselő elérhetőségei, ha van ilyen;
c) a személyes adatok tervezett kezelésének célja, valamint az adatkezelés jogalapja;
d) a 6. cikkely (1) bekezdésének f) pontján alapuló adatkezelés esetén, az adatkezelő vagy harmadik fél jogos érdekei;
e) adott esetben a személyes adatok címzettjei, illetve a címzettek kategóriái, ha van ilyen;
f) annak ténye, hogy az adatkezelő harmadik országba vagy nemzetközi szervezet részére kívánja továbbítani a személyes adatokat, továbbá a Bizottság megfelelőségi határozatának léte vagy annak hiánya, vagy a 46. cikkelyben, a 47. cikkelyben vagy a 49. cikkely (1) bekezdésének második albekezdésében említett adattovábbítás esetén a megfelelő és alkalmas garanciák megjelölése, valamint az azok másolatának megszerzésére szolgáló módokra vagy az azok elérhetőségére való hivatkozás.

Jogunk van továbbá tudni, meddig tárolják személyes adatainkat vagy, ha nincs pontos időtartam, milyen szempontok szerint határozzák meg a tárolás idejét. Kérhetjük az adatkezelőtől a személyes adatainkhoz való hozzáférést, azok helyesbítését, törlését vagy kezelésének korlátozását. Tájékoztatniuk kell bennünket arról, hogy panaszt nyújthatunk be a felügyeleti hatósághoz arról, hogy szabályon vagy szerződéses kötelezettségen alapul, esetleg szerződés kötésének előfeltétele-e a személyes adatok szolgáltatása, továbbá mik a következményei annak, ha nem adjuk meg ezeket az adatokat.

Érintettként jogunk van kérni, hogy az adatkezelő haladéktalanul helyesbítse adatainkat, illetve kérhetjük azok törlését is, ha azokra már nincs szükség ahhoz az eredeti célhoz,

amely érdekében gyűjtötték, ha visszavontuk a beleegyezésünket, vagy ha adatainkat jogellenesen kezelték. Ha az adatkezelő nyilvánosságra hozta az adatokat, „azokat törölni köteles, az elérhető technológia és a megvalósítás költségeinek figyelembevételével megteszi az észszerűen elvárható (technikai) lépéseket annak érdekében, hogy tájékoztassa az adatokat kezelő adatkezelőket, hogy az érintett kérelmezte tőlük a szóban forgó személyes adatokra mutató linkek vagy e személyes adatok másolatának, illetve másodpéldányának törlését" – fogalmaz a rendelet.

Kivételt jelent a fenti előírások alól, ha az adatkezelésre a véleménynyilvánítás szabadságához és a tájékozódáshoz való jog gyakorlása; a személyes adatok kezelését előíró, az adatkezelőre alkalmazandó uniós vagy tagállami jog szerinti kötelezettség teljesítése, illetve közérdekből vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlása keretében végzett feladat végrehajtása céljából; a népegészségügy területét érintő közérdek alapján, a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból és jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez van szükség.

Korlátozások

Korlátozni is lehet az érintettek fentebb felsorolt jogait „ha a korlátozás tiszteletben tartja az alapvető jogok és szabadságok lényeges tartalmát, valamint az alábbiak védelméhez szükséges és arányos intézkedés egy demokratikus társadalomban" – zárul a harmadik fejezet, melyben a védendő területek között a nemzetbiztonságot, honvédelmet, közbiztonságot említik, de szükség lehet korlátozásra „bűncselekmények megelőzése, nyomozása, felderítése vagy a vádeljárás lefolytatása, illetve büntetőjogi szankciók végrehajtása" esetén

ben. Szintén korlátozhatják az érintettek jogait „a bírói függetlenség és a bírósági eljárások védelme; a szabályozott foglalkozások esetében az etikai vétségek megelőzése, kivizsgálása, felderítése és az ezekkel kapcsolatos eljárások lefolytatása; a közhatalmi feladatok ellátásához kapcsolódó ellenőrzési vagy szabályozási tevékenység; az érintett védelme vagy mások jogainak védelme; polgári jogi követelések érvényesítése" esetében.

Az érintetteknek tájékoztatást kell kapniuk a korlátozásról, az adatkezelés céljáról, a kezelt személyes adatokról, az adatkezelőről, kivéve, ha a tájékoztatás hátrányosan befolyásolja a korlátozás célját.

Tájékoztatni kell az adatvédelmi incidensekről

A rendelet megszabja az adatkezelő és -feldolgozó feladatait is avégett, hogy a személyes adatok kezelése, tárolása, továbbítása biztonságos legyen. Ennek érdekében védenie kell informatikai rendszerét, számítógépeit, zárnia kell az irattárolásra szolgáló helyiséget. Szükség lehet még az adatok álnevesítésére, és tesztelni is kell a rendszereket. Ha minden biztonsági intézkedés betartása mellett is megtörtént a baj, azaz elloptak személyes adatokat, vagy azok kiszivárogtak, az adatkezelőnek értesítenie kell a felügyeleti hatóságot és az érintettet.

A felügyeleti hatóságnak 72 órán belül jelentenie kell az incidenst – kivéve, ha az valószínűsíthetően nem jár kockázattal a magánszemélyek jogaira és szabadságaira nézve –, ha ez nem történt meg, akkor indokolni kell a késedelem okát is. A bejelentéskor ismertetni kell az incidens jellegét, továbbá azt, hogy hány személyt és milyen típusú adatokat érint, ismertetni kell a várható következményeket, az adatvédelmi incidens orvoslására tervezett intézkedéseket, beleértve az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket is. Az adatvédelmi incidensről az érintetteket is tájékoztatni kell, kivéve, ha titkosítás miatt az adatok külső fél számára értelmezhetetlenek. Ha az érintettek egyenkénti értesítése aránytalan erőfeszítést jelent, akkor az adatvédelmi incidens tényét oly módon kell nyilvánosságra hozni, hogy az érintettek arról hatékonyan tájékozódjanak.

És a gyakorlat?

Átrágva magunkat a rendeleten, újra csak úgy véljük: félő, hogy az alapjában hasznos kezdeményezés és minden részletre kiterjedő szabályozás belefullad majd a bürokráciába, egyebek mellett azzal, hogy lehetőséget ad több felügyeleti szerv létrehozására, bár megszabja az ezek közötti viszonyt. Ami az adatvédelmi felelősök felkészítését illeti, májusban többen is szerveztek tanfolyamokat, ezeken főleg a közintézmények (számukra kötelező lesz a rendelet előírásainak betartása) képviselői vettek részt, sejthetően azért, hogy a rendelet formai követelményeinek eleget tegyenek, azaz május 25. után legyen olyan alkalmazottjuk, akinek van adatvédelmi tisztviselői képesítése, de e sorok írásakor (igaz, május 15. előtt) nem láttunk még olyan honlapot, amelyen közzétették volna adatvédelmi tisztviselő elérhetőségeit. Ami szűkebb pátriánkat illeti, intézményfenntartónknál, a Bihar Megyei Tanácsnál lapzártánk idején már készültek az adatvédelmi tisztviselő kinevezésére.

Fried Noémi Lujza