GDPR: General Data Protection Regulation

KÉSZÜLJÜNK AZ **ÚJ ADATVÉDELEMRE!**

Földesi Gábor

Egyre többet halljuk ezt a mozaikszót: GDPR. Ez az EU Általános Adatvédelmi Rendelete. Megint egy újabb leszabályozás? Pénzbehajtás? Féljünk tőle? Miért van erre szükség? Segíti a munkánkat? Hogy a kérdésekre választ kapjunk, összegyűjtöttük a tudnivalókat. A GDPR az év legfontosabb története az online marketingben. Nem maradt sok idő, ezért érdemes tudni róla, milyen világ következik. A rendeletet 2018. május 25-től kell alkalmazni.

A GDPR röviden az Európai Unió és a Tanács által elfogadott, a személyes adatok védelméről és az ilyen adatok szabad áramlásáról szóló rendelete,

más néven általános adatvédelmi rendelet (General Data Protection Regulation). A téma azért tart számot nagy közérdeklődésre, mert mindeddig a személyes adatok kezeléséről csak európai uniós irányelv szólt, azt pedig a tagállamok maguk – sokszor eltérő módon – ültették át. Mostantól fogva ez változni fog, mivel a GDPR közvetlen hatállyal rendelkezik, minden tagállamban kötelezően alkalmazandó. Ennél fogva minden tagállamban ez a rendelet lesz a legfontosabb szabályanyag a személyes adatok kezelése és védelme tekintetében, attól eltérni csak akkor lehet, ha azt maga a GDPR megengedi.

NINCS TÜRELMI IDŐ

A GDPR egyik újdonsága az elszámoltathatóság elve. Ez egyfajta fordított bizonyítási kényszert jelent. Lényegében nem a hatóságnak kell bebizonyítania, hogy nem felelünk meg az adatvédelmi szabályoknak, hanem nekünk kell bizonyítanunk a megfelelést. Tehát nem kell fináncokra számítani, inkább fentről szólnak le és kérik be a tanúsítványokat. Türelmi idő nincs. Az unió hagyott felkészülési időt a GDPR-rel érintetteknek, mivel azt már 2016 májusában kihirdették, azóta érvényes és hatályos.

MIT KELL TENNÜNK MÁJUSTÓL?

Megszűnik a most működő, a NAIH által vezetett adatvédelmi nyilvántartás, az egyes adatkezeléseket nem kell bejelenteni. Bejelentési kötelezettség keletkezik viszont az adatkezelő oldalán ún. adatvédelmi incidensek, azaz személyes adatokkal kapcsolatos jogsértések esetén, az adatkezelő általi tudomásszerzést követően haladéktalanul, de legkésőbb 72 órán belül. Kivétel ez alól, ha a személyes adatok megsértése „valószínűsíthetően” (ezt persze nehéz konkretizálni) nem okoz nagy sérelmet az érintettek számára. A bejelentést ilyenkor a NAIH felé kell megtenni. Az incidenssel érintett személyeket csak akkor kell értesíteni, ha az adatsértés számukra valószínűsíthetően nagy kockázatot jelent, pl. banki kódok kiszivárgása esetén. Ha az adatfeldolgozó észlel jogsértést, ő is köteles ezt bejelenteni, mégpedig az adatkezelő felé.

EGY HAGYOMÁNYOS WEBOLDAL ESETÉN IS FIGYELNI KELL

Nem a weboldal ténye számít, hanem az azon található „adatgyűjtő tartalom” megléte. Legyen

az akár egy Facebook Like-gomb vagy egy hírlevél-feliratkozás, de vannak kevésbé szemet szúró adatkezelések is, mint például egy forráskódba ágyazott követőkód. Ezeknél minden esetben személyes adatok juthatnak a vállalkozás birtokába, például egy hírlevélre történő feliratkozás során név, e-mail-cím biztosan. Ebben az esetben pedig már meg kell felelni a GDPR rendelkezéseinek.

MELYIK HATÓSÁG ELLENŐRIZ?

A már létező NAIH, azaz a Nemzeti Adatvédelmi és Információszabadság Hatóság a személyes adatok védelmének biztosításáért felelős hatóság, feladata a személyes adatok védelméhez való jog érvényesülésének ellenőrzése és elősegítése. Azaz Magyarországon a NAIH felel majd a GDPR betartatásáért, ellenőrzéseket folytathat le, az adatvédelmi szabályok megsértőit szankcionálhatja. Az adatkezelés magában foglal szinte minden, a személyes adatokon végzett cselekményt, így azok felvételét, gyűjtését, tárolását, különböző célokra történő felhasználását, továbbítását, módosítását, hogy csak néhány adatkezelési műveletet említsünk.

Nem lehet automatikusan, „kéretlenül" hírlevelet, direkt marketing anyagokat küldeni, a hírlevelek, reklámanyagok küldéséhez előzetes hozzájárulás szükséges. A hozzájárulás pedig a GDPR szerint csak tevőleges magatartással valósulhat meg. Ilyennek minősül, ha maga a weboldal látogatója pipálja ki a hozzájáruló négyzetet. Nem elfogadható például az a gyakorlat, amely szerint a négyzet már kipipált, és azt a látogató csak jóváhagyólag – vagy éppen figyelmetlenségből – úgy hagyja.

MI VONATKOZIK A SÜTIKRE?

A GDPR szerint a sütiazonosítók alkalmasak a természetes személyek azonosítására, így kiterjed rájuk a GDPR hatálya. A sütisávról, azaz a „cookie-k"-ról ezért egyértelmű és pontos tájékoztatást kell adni az oldal adatvédelmi tájékoztatójában, és a felhasználónak kifejezetten és egyértelműen hozzá is kell járulnia ahhoz, hogy az oldal cookie-kat használjon.

Sőt, lehetőséget kell adni neki arra is, hogy megváltoztassa döntését, azaz egy ponton úgy döntsön, a továbbiakban nem járul hozzá a cookie-k alkalmazásához.

MI TÖRTÉNIK, HA NEM FOGLALKOZUNK A GDPR-REL?

A nemtörődömséggel komoly bírságnak tesszük ki magunkat és a cégünket. Azért javasolt mindenkinek felülvizsgálnia és hatályosítania az adatkezelési gyakorlatát, mert a GDPR az eddigieknél sokkal szigorúbb szankcionálási eszközöket ad a nemzeti hatóságok (itthon a NAIH) kezébe: A bírság maximális mértéke 20 millió euró vagy az előző év világpiaci árbevételének 4 százaléka. A kettő közül a magasabb jelenti a felső határt. Természetesen a NAIH a konkrét bírság összegét számos tényezőtől teszi majd függővé, így figyelembe veszi a jogsértés súlyát, mértékét, az okozott sérelem nagyságát, illetve azt, hogy az gondatlanságból, szándékosságból, netán menthető nemtudásból fakad-e.

MILYEN ÜZENET KÜLDHETŐ A LÁTOGATÓNAK?

Magánszemélyek részére kizárólag előzetes hozzájárulás alapján jogszerű direkt marketing célú üzeneteket küldeni. Viszont a szabályok értelmében már a hozzájárulás kifejezett kérése is direkt marketingnek minősül, ha az üzenet fő lényegi tartalma a hozzájárulás kérése. Nagyon lényeges tehát a

megfogalmazás, ezért javasoljuk az adatvédelmi szakértő véleményének kikérését a kiküldés előtt. A személyes adatok bekérése a GDPR szerinti adatkezelésnek minősül, márpedig csak olyan jellegű és mennyiségű személyes adatot lehet kezelni, amely az adatkezelés céljához feltétlenül szükséges és arra alkalmas. Mindig csak a minimum adatkört lehet kezelni, amelyek felhasználásával a cél – amelyből az adatokat gyűjtik – már megvalósítható.

MILYEN CÍMRŐL KÜLDHETŐ MARKETINGLEVÉL?

Marketing e-mail bármilyen e-mail-címről küldhető, a lényeg abban áll, hogy az e-mailből egyértelműen kiderüljön, hogy ki az adatkezelő. Marketing e-mailek esetében ezen kívül minden esetben biztosítani kell a leiratkozás lehetőségét úgy, hogy az egyértelmű és könnyű legyen. A leiratkozás után a felhasználó e-mail-címét véglegesen törölni kell minden adatbázisból, és praktikus, ha ez nem igényel manuális beavatkozást, tehát automatikusan történik.

AMI A FELIRATKOZÁST ILLETI

A levelekre történő feliratkozásnál szükséges, hogy a feliratkozó személy proaktívan járuljon hozzá személyes adatai kezeléséhez, pl. beikszel egy négyzetet a hozzájárulás esetén. A hozzájárulás e szerint akkor megfelelő, ha tevőleges, tehát a feliratkozó személy maga pipálja ki a bejelölő négyzetet, mert így kizárt annak lehetősége, hogy a feliratkozó tekintete véletlenül átsiklik egy már bejelölt négyzet felett. A hozzájárulás azt a követelményt is állítja, hogy annak megfelelő tájékoztatáson alapulónak kell lennie. Emiatt javasolt a weblapon elhelyezni egy a weblapra, hírlevélre, illetve e-mailre vonatkozó adatkezelési tájékoztatóra mutató linket, valamint hasonló módon egy bejelölő négyzetet, amelyben a feliratkozó nyilatkozik, hogy a tájékoztatást megismerte. Fontos, hogy enélkül ne lehessen az e-mailre feliratkozni. Emellett a feliratkozónak külön hozzá kell járulnia, hogy részére direkt marketing útján hirdetéseket küldjenek – ez is a fent leírtak szerinti bejelölő négyzet elhelyezésével oldható meg.

WEBÁRUHÁZAS ADATBÁZIS ESETÉN

A webáruház adatbázisában szereplő adatokat nem szabad az adott ügylet befejezése után kezelni, azokat törölni kell az ügylet végeztével. Kivétel ez alól természetesen, ha az érintett személy kifejezett hozzájárulását adja személyes adatai más célú további tárolásához is. Jelenleg a leggyakrabban alkalmazott szabadforrású rendszerek a következőkre biztosítanak lehetőséget: rendelés követése, korábban megrendelt áruk újrarendelése, korábbi rendelések megtekintése. Ha ezeket kitöröljük, akkor ezek a maguktól értetődő, egyértelmű funkciók elvesznek. Az ügylet végeztét ezért definiálni kell.

HOGYAN KÉRHETIK AZ ADATAIK TÖRLÉSÉT?

Adatai törlését bárki az adatkezelőhöz címzett nyilatkozattal kérheti szóban, írásban, postai címen, e-mail-címen, weboldalon – célszerűen azon a fórumon, amelyen keresztül az adatok jogszerűen az adatkezelőhöz kerültek. Ezért is fontos, hogy az adatkezelő az adatvédelmi tájékoztatójában feltüntesse pontos elérhetőségeit.

KINEVEZETT ADATVÉDELMI TISZTVISELŐ

A GDPR által használt pontos kifejezés az „adatvédelmi tisztviselő”. Nem szükséges minden cégnek, csak a GDPR-ben meghatározott esetekben, vagyis közhatalmi szerveknél, az adatalanyok nagymértékű megfigyelése esetén (pl. vagyonvédelem), illetve különleges személyes adatok megfigyelése esetén (pl. kórház). Az adatvédelmi tisztviselő egyébként lehet akár alkalmazott, akár külső megbízott – a felelősség és a szakértelem miatt mindenképpen az utóbbit javasoljuk.

ADATVÉDELMI TÁJÉKOZTATÓ IS KELL

Mindenképpen külön adatkezelési tájékoztatót, adatvédelmi szabályzatot érdemes készíttetni jól látható, elkülönült formában. Így az érintettek részére alkalmas arra, hogy megállapítsák az őket érintő jogokat és kötelezettségeket. ■

Forrás:
7blog.hu