

Változnak az adatvédelmi szabályok

Adatvédelemmel kapcsolatos, konzultációval összekötött előadásra hívta meg a Mezőgazdasági Szövetkezők és Termelők Országos Szövetsége a tagszervezetei képviselőit március 28-án. Az előadást Kovács Melinda, a Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) adatvédelmi főosztályának munkatársa tartotta. A változások a tagszervezeteket is erősen érintik, elsősorban a haszonbérleti szerződésekkel kapcsolatosan, a földtulajdonosok adatainak kezelése miatt. De további szerződéses kapcsolatok is említhetők, mivel a vállalatok beszállítói-kereskedelmi kapcsolatait is új szemlélettel kell kezelni.

A Magyarországon jelenleg is hatályban lévő, 2011. évi CXII. törvény (infotörvény) nemzetközi összehasonlításban is szigorú követelményeket támaszt a természetes személyek adatait kezelő szervezetekkel szemben, továbbá a NAIH kiemelten ellenőrzi az adatkezelők megfelelését a törvények szempontjából, kezdte mondandóját Kovács Melinda. Az Európai Unió új általános adatvédelmi rendelete (General Data Protection Regulation – GDPR) május 25-én lép hatályba, és a magyarországi vállalatok számára is jelentős változásokat hoz magával az adatvédelem területén.

Az elmúlt két évtized legnagyobb szabású adatvédelmi szabályozásváltozása sok új elvárást fogalmaz meg az adatokat kezelő szervezetekkel szemben, teljesen új alapokra helyezi az adatok gyűjtését, felhasználását és megőrzését. A vállalatoknak számos új intézkedést kell végrehajtaniuk annak érdekében, hogy mindenben megfeleljenek a GDPR előírásainak. Ha egy szervezet a saját megítélése szerint már megfelel a jelenleg hatályos előírásnak, úgy a területet szabályozó új uniós jogszabály nem jelent számára érdemi változást. Ebben az esetben nagy könnyebbség, hogy nem a nulláról kell építkezni, de így

is mindenkinek hoz újdonságot az új jogszabály, amire érdemes időben felkészülni.

A nyilvántartás-vezetési kötelezettség nem vonatkozik a 250 főnél kevesebb alkalmazottat foglalkoztató vállalkozásokra vagy szervezetekre – kivéve, ha az általuk kezelt adatok az érintettek jogaira és szabadságára nézve valószínűsíthetően kockázatot jelent. Kivételt jelent az is, hogyha az adatkezelés nem alkalmi jellegű, vagy ha az adatkezelés kiterjed a személyes adatoknak a 9. cikk (1) bekezdésében említett különleges kategóriáira vagy a 10. cikkben említett, a büntetőjogi felelősség megállapítására vonatkozó határozatokra és a bűncselekményekre vonatkozó személyes adatok kezelésére.

Az alapelvek legfontosabb változása az a szemléletváltás, ami az elszámoltathatóság elvén fogalmazódott meg. Megfordították a bizonyítás terhét, ami azt jelenti, hogy az adatok jogszabályoknak megfelelő kezelését az adatkezelő köteles bizonyítani. Tehát az adatkezelő a felelős a személyes adatok kezelésére vonatkozó, a rendelet 5. cikke (1) bekezdése szerinti elveknek való megfelelésért, továbbá képesnek kell lennie a megfelelés igazolására. Lényegében az elszámoltathatóság elvéhez

kapcsolódik a beépített adatvédelem elve, és az alapértelmezett adatvédelem is, mondta Kovács Melinda.

Az alapelvek lényeges tartalmát tekintve azonban nem történt jelentős változás, hangsúlyozta az előadó. A nyilvántartási kötelezettség esetében fontos könnyítésnek tűnhet, hogy a rendelet hatályba lépését követően megszűnik az adatkezelők kötelező bejelentkezési kötelezettsége az adatvédelmi nyilvántartásba. Ugyanakkor május 25-étől minden szervezetnek saját magának kell átlátható formában vezetnie és szükség esetén a hatóság rendelkezésére bocsátania személyes adatkezelési tevékenysége nyilvántartását. Az adatkezelési tevékenység hiánytalan felmérése komoly erőforrásokat igényelhet a szervezetek részéről.

Bár a jogalapok terén sincsenek változások a koncepcióban, fontos szigorítás a hozzájárulás alapján történő adatkezelés feltételeinek szigorítása, mivel a hozzájárulásnak minden körülmények között önkéntesnek és visszavonhatónak kell lennie. Így számos esetben szükség lehet az adatkezelés újfajta jogalapjának meghatározására (egyebek között a munkavállalók adatainak kezelésében). Érdemes kidolgozni egy saját, az ágazat speciális helyzetéhez igazodó, annak sajátosságait figyelembe vevő, az adatvédelmi szabályokat tartalmazó brosúrát, amelyben a kötelező vállalati szabályokat és szerződéses rendelkezéseket rögzítik. Ezt a szabályozást kell az érintettekkel dokumentált körülmények között ismertetni.

Kovács Melinda kitért az érintettek jogainak változásaira is. A rendelet felsorolja, milyen jogok illetik meg azokat a személyeket, akiknek az adatait kezelik. Ezek a megerősített jogok lehetővé teszik a természetes személyek számára,



hogy szabadabban rendelkezzenek személyes adataikról azáltal, hogy egyértelműen hozzájárulásukat kell adniuk személyes adataik kezeléséhez, továbbá ezáltal könnyebben hozzáférhetnek a személyes adataikhoz, és rendelkezhetnek a személyes adatok helyesbítéséről, tárolásuk megszüntetéséről és törléséről. Az adataikat megosztó személyeknek joguk van az adatkezelés kifogásolásához, a többi között a személyes adatok profilalkotás céljából történő felhasználására vonatkozóan, valamint joguk lesz az adatok szolgáltatók közötti hordozásához is. A rendelet emellett kimondja, hogy az adatkezelők kötelesek átlátható és könnyen hozzáférhető információkat nyújtani az érintetteknek a személyes adataik kezelésével kapcsolatban, mondta el Kovács Melinda.

Itt kell megemlíteni azt is, hogyan továbbíthatóak a személyes adatok a harmadik országokban, ugyanis a rendelet ezt is szabályozza. A rendelet továbbá felhatalmazza az Európai Bizottságot, hogy értékelje a harmadik ország adott régiójában vagy adatkezelő ágazatában biztosított adatvédelem szintjét. Ha a Bizottság nem hoz határozatot az adatvédelem szintjének megfelelőségéről, akkor a személyes adatokat csak különleges esetben, illetve megfelelő biztosítékok felmutatása esetén lehet továbbítani.

Az infotörvény és a rendelet egyik legfontosabb különbsége, hogy a rendeletben előírják a személyes adatokat érintő incidensek 72 órán belüli kötelező bejelentését az adatvédelmi hatóságnak, a NAIH-nak, jelentette ki az előadó. Így mindenképpen szükség van azokra az eljárásokra, amelyek az incidensek bejelentéséhez biztosítják a szükséges információkat. Az adatvédelmi incidensek bejelentésének kezelésére jogászokból és informatikusokból álló főosztályt hoz létre a hatóság. Az incidensbejelentési kötelezettség bevezetésével együtt előírják a szervezeteknek, hogy tudatosan csökkentsék az adatvédelmi incidensek bekövetkezésének valószínűségét, valamint ha mégis történik ilyen eset, mindent tegyenek meg a természetes személyeket fenyegető kockázatok csökkentése érdekében.

A rendelet szintén május 25-étől valamennyi újonnan megkezdett, potenciális kockázatot jelentő adatkezelési tevékenység esetére előírja adatvédelmi hatásvizsgálat elvégzését. Bár a rendelet szövege szerint a hatályba lépését megelőzően nem kell ilyen végezni, a hatásvizsgálat lefolytatására vonatkozó eljárásrendnek és procedúrának addigra rendelkezésre kell állnia. Éppen ezért, saját magunk és a hatóság megnyugtatása érdekében célszerű felülvizsgálni, hogy zárt-e az informatikai környezetünk, és hogy elég hatékonyak-e a szervezeti és a technikai intézkedések. Habár informatikai rendszerek esetén nem beszélhetünk 100 százalékos biztonságról, de nemcsak a hatóság, hanem az ügyfeleink bizalmának megőrzése érdekében is minden elvárható meg kell tennünk a ránk bízott személyes adatok védelme érdekében.

A rendelet részletesen ismerteti az adatkezelőkre és az adatfeldolgozókra háruló kötelezettségeket, mondta az előadó. Ezek magukba foglalják olyan biztonsági intézke-

Az általános adatvédelmi rendelet lehetővé teszi az adatok szabad áramlását az egységes digitális piacon, az eddiginél jobban védi az európaiak magánélethez való jogát, erősíti a fogyasztók bizalmát és biztonságát, ugyanakkor új lehetőségeket nyit meg a vállalkozások, különösen a kisebb cégek előtt. Bár az új rendelet minden tagállamban közvetlenül alkalmazandó szabályokat határoz meg, bizonyos tekintetben további jelentős alkalmazkodást igényel. Például az uniós tagállamok kormányainak egyes hatályos jogszabályokat módosítaniuk kell, illetve az adatvédelmi hatóságoknak létre kell hozniuk az Európai Adatvédelmi Testületet. A Bizottság 1,7 millió eurót szán az adatvédelmi hatóságok finanszírozására és adatvédelmi szakemberek képzésére. További 2 millió euró fordítható a nemzeti hatóságok vállalkozásokat – különösen kkv-eket – segítő tevékenységének támogatására.

Frans Timmermans első alelnök így nyilatkozott a témában: „Az általunk javasolt rendelkezések kiegészítik az EU adatvédelmi keretszabályait. Korszerű és hatásos adatvédelmi szabályokról gondoskodnak az elektronikus hírközlés területén, amelyek biztosítják, hogy az európai uniós intézményekre ugyanolyan magas szintű normák legyenek érvényesek, mint amilyeneket a tagállamoktól elvárunk.”

Andrus Ansip, az Európai Bizottság egységes digitális piacért felelős alelnöke a következőket mondta: „Digitális jövőnknek csak a bizalomra alapozva építhetjük. Minden ember magánélethez való jogát védeni kell. Május 25-én életbe lépnek a megszilárdított uniós adatvédelmi szabályok. Nagy előrelépés ez, és eltökélt szándékunk, hogy minden érintett számára sikerré tesszük a váltást.”

Věra Jourová, a jogok érvényesüléséért, a fogyasztóvédelmért és a nemek esélyegyenlőségéért felelős biztos úgy fogalmazott: „Gazdaságunk jövője és személyes biztonságunk tekintetében is meghatározó szerepe van annak, hogy hogyan kezeljük az adatokat. Annak érdekében, hogy reagálni tudjunk az új kockázatokra, korszerű szabályokra van szükség. Ezért felszólítjuk az uniós kormányokat, hatóságokat és vállalkozásokat, hogy a közelgő nagy napig rendelkezésükre álló időt minél jobban használják ki, készüljenek fel, és végezzék el a rájuk háruló feladatokat.

A korszerűsített szabályok nemcsak az európai polgárok személyes adatainak jobb védelmét szolgálják, hanem egyúttal új lehetőséget kínálnak az adatok áramlására a ténylegesen egységes digitális piacon, és nagyobb rugalmasságot tesznek lehetővé a vállalkozásoknak az innovációban. Az EU-ban egységesen érvényes szabályok bevezetése várhatóan jelentős megtakarítást és az eddiginél jobb jogbiztonságot hoz a vállalkozásoknak, mivel nem 28 különböző szabályozásnak kell megfelelniük és egy széttagolt piacon helytállniuk. Emellett az új szabályok több rugalmasságot biztosítanak a kis- és középvállalatoknak. Világszinten etalonnak tekinthető adatvédelmi normákat vezetünk be. Büszke vagyok arra, hogy adatvédelmi szabályaink egyre inkább referenciaként és inspirációként szolgálnak más országok és regionális szervezeteknek a maguk adatvédelmi jogszabályainak megalkotásához vagy módosításához. Ma és holnap egyre nagyobb mértékben az határozza meg gazdaságunk jövőjét és személyes biztonságunkat, hogy hogyan kezeljük az adatokat. Jól tesszük, ha felkészülünk, ha komolyan vesszük az e téren felmerülő kockázatokat, és ha élünk az adódó lehetőségekkel.”

dések végrehajtásának kötelezettségét, amelyek arányosak a végzett adatkezelési műveletekkel járó kockázattal. Az adatkezelőknek bizonyos esetekben be kell jelenteniük a személyes adatok biztonságának sérülését.

Egyébként minden hatóságnak ki kell neveznie egy adatvédelmi tisztviselőt, és hasonló kötelezettség vonatkozik azokra a vállalkozásokra is, amelyek kockázatos adatokat kezelnek.

Kovács Melinda kitért a

szankciókra is, ugyanis a rendelet a jogsértések típusa szerint határozza meg a maximálisan kiszabható bírság összegét. Nagyon szigorú szankciókat szabtak meg az adatvédelmi szabályokat megsértő adatkezelőkkel és adatfeldolgozókkal szemben. Az adatkezelőkre kiróható büntetés akár 20 millió forint vagy éves árbevételük 4 százaléka is lehet. A közigazgatási szankciókat a tagállam adatvédelmi hatósága szabja ki. A GDPR által kilátásba helyezett 20 millió forintos bírság magyarországi alkalmazására várhatóan nem kerül sor, mert a hatóságnak nem az a célja, hogy a működő vállalatokat ellehetetlenítse. A NAIH a rendelet hatályba lépésének idejére szakértői gárdája létszámának bővítésével készül.

Összegzőképpen elmondható, hogy a személyes adatok kezelését jogszerűen és tisztességesen, az érintett számára átlátható módon kell végezni. A személyes adatok gyűjtése csak egyértelműen meghatározott, jogszerű célból történhet, és ezekkel a célokkal nem összeegyeztethetően nem kezelhetők. A személyes adatoknak az adatkezelés célja szempontjából relevánsnak kell lenniük, és a feltétlenül szükséges információkra kell korlátozni a körüket. A személyes adatoknak pontosnak, és szükség esetén naprakésznek kell lenniük, a pontatlan személyes adatokat haladéktalanul helyesbíteni, illetve törölni kell. A személyes adatokat olyan formában kell tárolni, amely az érintettek azonosítását csak a személyes adatok kezelési céljainak eléréséhez szükséges ideig teszi lehetővé (ez a határidő eléggé tág). A személyes adatokat olyan módon kell kezelni, hogy megfelelő technikai vagy szervezeti intézkedésekkel elérhető legyen a biztonságuk, ide értve a jogosulatlan vagy jogellenes kezelésükkel, véletlen elvesztésükkel, megsemmisítésükkel, károsodásukkal szembeni védelmet.

H. GY.