Adatvédelmi Kisokos

crosssec.com

01

crosssec solutions

Impresszum

Kiadja / Crosssec Solutions Kft. 1052 Bp., Deák Ferenc tér. 3.

Tel.: +36 20 666 7894
crosssec.com
info@crosssec.com

Szerző / Dr. Káldi Ivett

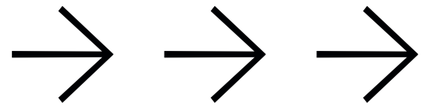
Design / Mezei Gréta

Közreműködött / Gátos Eszter, Győri Aletta,
Kovács Marcell, Mátyus Lilla, Szűcs Zsolt

A kiadvány jelen változata
készült: 2021. május

Adatvédelmi Kisokos 01 / 2021

Tartalomjegyzék



Miért is született meg az Adatvédelmi Kisokos?

Adatvédelem, GDPR... Sokunkban még mindig homályos a kép arról, mit is jelentenek, mit is kellene kezdeni velük. Ne tarts tőlük, ismerd meg – mi segítünk alaposan körbejárni őket!

→ → →

Az adatvédelem és GDPR szavak hallatán sokunkban még mindig egy homályos kép jelenik meg azzal kapcsolatban, hogy pontosan mit is takarnak ezek a kifejezések. A GDPR a General Data Protection Regulation, azaz az Általános Adatvédelmi Rendelet angol rövidítése. A rendelet a természetes személyek adatainak kezelésével összefüggő egységes szabályokat és elveket fogalmaz meg és az uniós polgárok személyes adatait hivatott védeni: szabályozza többek között az adatgyűjtés módját, feldolgozását, tárolását, törlését, az adatok továbbítását és felhasználását. Minden vállalkozásnak, amely Európában üzleti tevékenységet folytat vagy uniós polgárok személyes adatait kezeli, meg kell felelnie e szabályozásnak.

Laikusként gyakran elveszünk az adatvédelmi szabályok rengetegében, nem tudjuk igazán értelmezni a sokszor száraz jogi megfogalmazások mögötti valódi jelentéstartalmat. Kisvállalkozóként vagy akár egy nagyobb cég vezetőjeként kezdetben talán elhárítottuk magát a gondolatot is, hogy az adatvédelmi előírásoknak való megfelelésbe energiát fektessünk, aztán az idő múlásával mégis megtettük azokat a lépéseket, amelyek feltétlenül szükségesek az adatvédelmi szempontból is megfelelő és megbízható működésnek.

Miért is született meg az Adatvédelmi Kisokos?

—

Az internetet böngészve nagyon sok információt találunk az adatvédelemről, azonban bátran kijelenthetjük, hogy kevés a téma olyan igazán közérthető, gyakorlatias megközelítése, amely kicsit elszakad a hivatalos, definíciószerű magyarázattól és életszerű képet tár elénk. Minden szakterület próbálja a maga szemszögéből legfontosabb információkat összegyűjteni, egy helyre összefűzni az érdeklődők számára. Ügyvédi irodák, adatvédelmi szakjogászok, IT-szakemberek, HR-es kollégák, marketinggel foglalkozó weboldalak, illetve maga a magyar adatvédelmi hatóság is rengeteg hasznos információval szolgál az adatvédelmi témakörben kutakodók számára. Nem igazán találunk azonban olyan kompakt anyagot, amely e szerteágazó témaköröket egy csokorba szedi; ami végigkalauzol minket az adatvédelmi szabályozás rendszerén: milyen jogforrások szabályozzák ezeket a kérdéseket, miről is szól lényegében az adatvédelmi rendelet, hol találkozhatunk a mindennapjainkban ezekkel a rendelkezésekkel, kérdésekkel, mire kell figyelnünk alkalmazottként, cégvezetőként, milyen kézzelfogható és hétköznapi, gyakorlatias példák segíthetnek minket mindezek megértésében és hogyan is kerülhetnénk közelebb ehhez az egészhez?

Fentiek alapján Adatvédelmi Kisokos című, három részes kiadványsorozatunkkal szeretnénk segítséget nyújtani az adatvédelem iránt érdeklődőknek, az adatvédelemmel esetleg már aktívan foglalkozó Olvasóinknak, mindezt könnyed, olvasmányos nyelvezettel.

Kiadványunk első részében megismerhetjük az adatvédelem fontosabb fogalmait, szabályozási rendszerét, alapvetéseit, az „érintettek” jogait, az adatkezelés jogalapjait. A második részben a sokunkat érintő kis- és középvállalkozások, a munkahelyi adatkezelés, a reklámok és cookiek kerülnek rivaldafénybe. Cikksorozatunk lezárásaként pedig bepillantást nyújtunk a Facebook világába, és több érdekes területre, például az egészségügyi, ügyvédi adatkezelésbe, a pénzmosási törvénytől kezdve a postai küldeményeken át a villamoson készült kamerafelvételek kérdéseibe.

Reméljük, hogy a kérdezz-felelek formában íródott anyagot mindenki – akár adatkezelői, akár érintetti oldalon – magáénak érzi és ötleteket merít belőle,
növelve ezzel adatvédelmi tudatosságát.

Az adatvédelmi szabályozás rendszere

Kezdjük az alapokkal: Mi is az a GDPR, miről szól az Info-törvény és a kiegészítő gyűjtemény, a „salátatörvény”? Mivel foglalkozik, miben segít és miért bírságol a NAIH?

→ → →

02.1

Általános Adatvédelmi Rendelet (GDPR)

A GDPR /General Data Protection Regulation/ az Európai Unió általános adatvédelmi rendelete, teljes megnevezése szerint az Európai Parlament és a Tanács /EU/ 2016/679 Rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről.

A GDPR úttörőnek számít abból a szempontból, hogy rendelkezéseit közvetlenül, tagállami átültetés nélkül kell alkalmazni. Az itt említett, hatályon kívül helyezett 95/46/EK rendelet tulajdonképpen egy irányelv volt. Ezt ültették át a tagállamok a saját jogrendjükbe, így tehát saját nemzeti jogszabályaikat alkalmazták. Ezt a rendszert változtatta meg gyökereiben a GDPR, ami az előbbiekkel ellentétben több tízmillió közvetlen címzettnek – adatkezelőnek, adatfeldolgozónak szól. Maga a jogszabály 2016. május 25-én, kötelező alkalmazása azonban – kétéves türelmi időt követően – 2018. május 25. napján lépett hatályba.

02.2

Infotörvény

Az „Infotörvényként” emlegetett jogszabály a 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról.

Ahogyan kihirdetése évszámából is láthatjuk, kerek egy évtizede lépett életbe, amit azonban jelentősen átformált a GDPR megszületése. Az Infotörvény szóban forgó módosítását az eredetileg tervezett időponthoz képest néhány hónapos csúszással, 2018. július 25-én hirdették ki és másnap lépett hatályba. De pontosan melyek a különbségek, illetve a kapcsolódási pontok az információs önrendelkezési jogról és az információszabadságról szóló magyar törvény és az Európai Unió GDPR-rendelete között? – a későbbiekben ezt is eláruljuk.

Adatvédelmi Kisokos 01 / 2021

02.3

GDPR „salátatörvény”

Az Európai Unió adatvédelmi reformjának végrehajtása érdekében szükséges törvénymódosításokról szóló 2019. évi XXXIV. törvény.

A köznyelvben csak GDPR „salátatörvényként” elhíresült törvény tulajdonképpen egy csokorba gyűjti azt a 86(!) jogszabályt, amelyeket a GDPR közvetlenül érint, amelyekre közvetlen hatással van – a Munka Törvénykönyvétől a légiközlekedésen át egészen a lakcímnyilvántartás szabályozásáig.

02.4

Nemzeti Adatvédelmi és Információszabadság Hatóság

A sokunk által már ismert Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) a független magyar adatvédelmi hatóság, amely nem csupán bírságok kiszabásával foglalkozik, hanem sokrétű feladatai közt útmutatókkal is szolgál az adatvédelem területén felmerülő kérdések, problémák megoldásában. A NAIH internetes oldalán kalandozva rengeteg bogarászásra érdemes, hasznos információt találunk az adatvédelem uniós és nemzeti szabályozásáról, jogesetekről, állásfoglalásokról, határozatokról, aktuális hírekről.

Gyakran ismételt kérdések

Sorra vesszük a fogalmakat: adatkezelés, személyes adat, az érintettek jogai, adatvédelem, incidensek. Majd tisztázzuk az összes fontos kérdést, ami csak egy cégnél e körben szóba kerülhet.

→ → →

#01
Mi is az a GDPR?

Az alábbiakban a GDPR-rendelettel összefüggő legfontosabb kérdésköröket összegyűjtve ismerkedhetünk meg az adatvédelmi szabályozás alappilléreivel.

#02
Kire vonatkozik?

A GDPR hatálya alá tartozik minden természetes vagy jogi személy (cég, egyéni vállalkozó is például), közhatalmi szerv, ügynökség vagy bármely egyéb szerv, aki vagy amely személyes adatot kezel.

#03
Mit jelent az adatkezelés?

Az adatkezelés magába foglal szinte minden, személyes adatokon végzett cselekményt, így azok felvételét, gyűjtését, tárolását, különböző célokra történő felhasználását, továbbítását, módosítását, hogy csak néhány adatkezelési műveletet említsünk.

#04
Mi a különbség az adatkezelő és az adatfeldolgozó között?

A fentiekben körülírt adatkezelést végző szervezet (akár cég vagy egyéni vállalkozó) az Adatkezelő. Az Adatkezelő megbízásából és nevében személyes adatokkal dolgozó, általában harmadik fél az Adatfeldolgozó. A fontos különbség, hogy míg az adatkezelő meghatározza az adatkezelés célját, eszközeit, módszereit is, azaz dönt az adatok sorsáról, addig az adatfeldolgozó csak az adatkezelő utasításai alapján az adatkezelő nevében végez – jellemzően technikai – műveleteket az adatokon (pl. webtárhely szolgáltatója).

#05
Hol kell alkalmazni a GDPR-t?

A GDPR mint uniós rendelet, az Unióhoz valamilyen okból kapcsolódó adatkezelésekre állapít meg szabályokat. Így alkalmazni kell a GDPR-t, ha az Ön vállalkozása, cége tevékenységét az Unió területén belül fejti ki, és az adatkezelés e tevékenységével összefügg. Ám a GDPR továbbmegy ennél: alkalmazandó ugyanis azokra az adatkezelésekre, adatfeldolgozási műveletekre is, amelyeket az Unióban tevékenységi hellyel ugyan nem rendelkező adatkezelő vagy adatfeldolgozó végez, ha áruknak vagy szolgáltatásoknak az Unióban tartózkodó érintettek számára történő nyújtásához, vagy az érintettek Unió területén belül tanúsított viselkedésének megfigyeléséhez kapcsolódnak.

Az árukat vagy szolgáltatásokat abban az esetben nyújtják az EU-ban tartózkodó érintettek számára, ha az áru vagy szolgáltatás nyújtása során kifejezetten nevesítik az EU-t vagy egy tagállamot, az adatkezelő vagy adatfeldolgozó kifejezetten az EU területén tartózkodó személyek részére hirdeti az árut vagy szolgáltatást, az adatkezelő vagy adatfeldolgozó tevékenységének nemzetközi jellege megfigyelhető, kifejezetten tagállami vagy uniós kiterjesztésű domain nevek alkalmazása („.hu” vagy „.eu”), nemzetközi ügyfélkör említése, nemzeti nyelv vagy az árak nemzeti valutában történő feltüntetése, a tagállamban történő kiszállítás.

A megfigyelés pedig akkor irányul az EU területén tartózkodó adatalanyokra, ha az adatkezelés viselkedésalapú reklámozást, helymeghatározó szolgáltatást, cookie-k segítségével történő online megfigyelést, személyre szabott étkezési vagy egészségügyi tanácsadást, zártláncú megfigyelőrendszert, piackutatást, az érintett egészségi állapotának megfigyelését foglalja magában.

Adatvédelmi Kisokos 01 / 2021

„ ...a személyes adat gyakorlatilag bármi lehet, ami csak egy emberhez köthető,... ”

#06
Mit is értünk személyes adat alatt?

Azonosított vagy azonosítható természetes személyre (az “érintettre”) vonatkozó bármely információt. 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.

Tehát nem csak az alapján azonosítható valaki, ha ismertek a természetes személyazonosító adatai: a neve, a születési helye és ideje, illetve az anyja neve, esetleg a lakcíme. Úgy is lehet, ha csak annyi adatot ismerünk, hogy a középső lépcsőházban élő magas szemüveges nő. Így a személyes adat gyakorlatilag bármi lehet, ami csak egy emberhez köthető, mint az éttermi fogyasztás, a gépjármű márka, az alkalmassági teszt eredménye, a gépjármű fogyasztása, a cookie, az IP-cím stb.

#07
Nekem is van különleges személyes adatom?

A személyes adatok szigorúbb megítélés alá eső fajtái az úgynevezet különleges, más néven kiemelt személyes adataink: faji vagy etnikai származásunkra, politikai véleményünkre, vallási vagy világnézeti meggyőződésünkre, szakszervezeti tagságunkra utaló személyes adatok, valamint az egyedi azonosításunkat célzó genetikai és biometrikus, a szexuális irányultságunkra vonatkozó, illetve esetlegesen bűnügyi adataink. Ezek kezelése alapesetben TILOS a GDPR rendelkezései szerint, azonban vannak kivételek. Személyes azonosítást célzó orvosi vizsgálat lehet például egy vérvizsgálat, ami természetesen nem tilos, ha hozzájárulunk. A hozzájárulásunk egyébként egy tipikus formája annak, hogy jogszerűvé váljon az ilyen érzékeny adatok kezelése is. A hozzájárulásunknak azonban mindig kifejezettnek kell lennie.

#08
Profilozunk, profilozunk...

Profilalkotásról akkor beszélünk, amikor személyes adatokkal valamilyen formájú automatizált kezelés történik, amelynek a célja egy ember vagy embercsoport személyes jellemzőinek értékelése. A személyes jellemzők alapján csoportokba sorolhatnak minket, majd elemzik viselkedésünket és előrejelzéseket készítenek például érdeklődési körünkről, várható magatartásunkról, szokásainkról.

A profilalkotás különleges kategóriájú adatokat hozhat létre olyan adatokból is, amelyek önmagukban nem minősülnek annak, de azzá válnak, ha más adatokkal összekapcsolják őket. Például elképzelhető, hogy következtetni lehet valaki egészségi állapotára, ha az élelmiszervásárlási előzményeit összekapcsolják az élelmiszerek minőségére és energiatartalmára vonatkozó adatokkal.

Érdekességként említhetjük azt a tanulmányt, amely összekapcsolta a Facebook „lájkokat” egy felmérés adataival, és megállapította, hogy a kutatók pontosan előrejelezték a férfi felhasználók szexuális orientációját az esetek 88%-ában, a felhasználók etnikai származását az esetek 95%-ában, azt pedig, hogy a felhasználó keresztény vagy muszlim, az esetek 82%-ában. [1]

[1] Forrás: https://www.pnas.org/content/110/15/5802

#09
...aztán automatizált döntést hozunk?

Nem feltétlenül ugyan, de a profilozás és az automatizált döntések gyakran kéz a kézben járnak. Az automatizált döntéshozatal az a képesség, hogy az adatkezelők technológiai eszközök segítségével, emberi beavatkozás nélkül hoznak döntéseket. Az automatizált döntések alapulhatnak bármilyen adaton, például: egy kérdőívre adott válaszon, egy alkalmazás révén gyűjtött helymeghatározási adaton, hitelminősítési pontszámon. Gyorshajtási bírság kiszabása pusztán a sebességmérő kamerákból származó bizonyítékok alapján automatizált döntéshozatali folyamatnak minősül, amely nem feltétlenül jár profilalkotással. Azonban profilalkotáson alapuló döntéssé válik, ha az idők folyamán figyelemmel kísérik a természetes személy vezetési szokásait, és például a kiszabott bírság összege olyan más tényezőkre is kiterjedő értékelés eredménye, mint például, hogy a gyorshajtás ismétlődő szabálysértés-e, vagy hogy a vezető a közelmúltban elkövetett-e más közlekedési szabálysértést.

#010
Mi a helyzet az „otthoni” adatkezelésekkel?

Joggal felmerülhet bennünk a kérdés, mi a helyzet akkor, ha kizárólag a saját személyes tevékenységeink során, otthon kezelünk személyes adatokat? Van egy nyilvántartásom az összes ismerősöm születésnapjáról, esetleg a barátaim lakcíméről, telefonomban rengeteg telefonszám, e-mail cím található. Ebben az esetben ránk nem vonatkozik a GDPR, azt ezekre az adatkezelésekre nem kell alkalmaznunk. Azonban vigyázzunk, mert ha például egyéni vállalkozóként kezelünk személyes adatokat, már más a helyzet – de erről a későbbiekben még szólunk.

#011
Honnan tudom, hogy jogszerűen kezelik-e az adataimat?

A GDPR felsorolja azokat a jogalapokat, amelyek megléte esetén jogszerű az adatkezelés. A négy legfontosabb jogalap a személyes adatok kezelésére: a hozzájáruláson alapuló, a szerződésen alapuló, a jogi kötelezettségen alapuló, és a jogos érdeken alapuló. A GDPR-ban rögzített további két jogalap – a közérdekű feladat végrehajtása és az érintett érdekeinek védelme – gyakorlati jelentőséggel kevésbé bír, mint az előbbiek.

Meglehetősen gyakori például, hogy a foglalkoztatási jogszabályok olyan jogi kötelezettségeket írnak elő a munkáltató számára, amelyek személyes adatok kezelését teszik szükségessé (például az adó kiszámításához és a munkabér kezeléséhez). Egyértelmű, hogy ilyen esetekben az adott jogszabály az adatkezelés jogalapjául szolgál.

Ha több jogalap áll rendelkezésünkre, választanunk kell közülük, amely választásnál körültekintően kell eljárni, hiszen hatással lehet az adatkezelésre.

#012
Aláírt formanyomtatványtól az elektronikus jelölőnégyzetekig
– avagy milyen egy megfelelő érintetti hozzájárulás?

„ Az adatkezelésre jogalapot szolgáltató hozzájárulás bármikor visszavonható, ellentétben például a szerződésen alapuló adatkezeléssel, ahol ez nem mondható el. ”

Az érintett hozzájárulása az akaratának önkéntes, konkrét, megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet (ráutaló magatartás) útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez. A hallgatás, az előre bejelölt négyzet vagy a nem cselekvés nem minősül hozzájárulásnak.

Egy mobiltelefonos képszerkesztő alkalmazás arra kéri a felhasználóit, hogy szolgáltatásai igénybevételéhez aktiválják GPS-lokalizációjukat. Az alkalmazás azt is közli a felhasználóival, hogy a gyűjtött adatokat viselkedésalapú hirdetésekhez fogja felhasználni. Sem a földrajzi helyzetmeghatározás, sem az online viselkedésen alapuló hirdetés nem szükséges a képszerkesztő szolgáltatás nyújtásához, és mindkettő túlmutat a nyújtott alapszolgáltatás teljesítésén. Ám ha a felhasználók az ezekhez a célokhoz való hozzájárulás nélkül nem használhatják az alkalmazást, a hozzájárulás nem tekinthető önkéntesnek.

Az érintetti hozzájárulás meglétét kérdéses helyzetben az adatkezelőnek kell bizonyítania. Különböző célú adatkezelésre külön-külön be kell szerezni az érintett hozzájárulását, minden célhoz tartoznia kell egy jogalapnak:

Egy kábeltelevízió-hálózat az előfizetői hozzájárulása alapján gyűjti a személyes adataikat annak érdekében, hogy személyes javaslatokat tárhasson eléjük olyan új filmekkel kapcsolatban, amelyek iránt a televíziózási szokásaik alapján esetlegesen érdeklődhetnek. Egy idő elteltével a televízióhálózat úgy dönt, hogy szeretné harmadik felek számára lehetővé tenni, hogy az előfizető televíziózási szokásai alapján célzott hirdetéseket küldjenek (vagy jelenítsenek meg). Ezen új cél miatt például új hozzájárulásra van szükség.

Az adatkezelésre jogalapot szolgáltató hozzájárulás bármikor visszavonható, ellentétben például a szerződésen alapuló adatkezeléssel, ahol ez nem mondható el.

#013
Mit jelent a szerződésen alapuló adatkezelés?

Erre a jogalapra akkor támaszkodhat egy adatkezelő, ha:

01 ***az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél, vagy***

02 ***az adatkezelés a szerződés megkötését megelőzően, az érintett kérésére történő lépések megtételéhez szükséges.***

A jogalap alkalmazásának előfeltétele tehát, hogy a kérdéses szerződés kapcsán az érintett szerződő fél legyen vagy a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez legyen szükség az adatkezelésre.

Figyeljünk továbbá arra is, hogy ez a jogalap csak a szerződés fennállása idején hivatkozható, a szerződés megszűnése esetén jogalapot kell váltanunk. A jogalap tehát csak arra vonatkozik, ami a szerződés teljesítéséhez szükséges, így nem vonatkozik a nemteljesítés által előidézett további lépésekre (például kölcsönszerződés felmondása fizetési késedelem miatt), illetve a szerződés végrehajtásakor felmerülő egyéb eseményekre (például kölcsönszerződés felmondása).

#014
Jogos érdek, mint a Jolly Joker jogalap?

A jogos érdek fogalma meglehetősen tágan értelmezhető az adatkezelés vonatkozásában, ami akár könnyelműségre is okot adhat. Ha egy adatkezelésnek a jogos érdek a jogalapja, ez aránylag egy nagyobb mértékű szabadságot adhat az adatkezelő számára. Nem köti ugyanis a fentiekben részletezett szerződés érvényessége, hatályossága, az érintett hozzájárulása, a jogszabályi felhatalmazás megléte. Azonban a “mindennek megvan az ára” elv mentén ez jár a legnagyobb adminisztratív teherrel, az ún. érdekmérlegelési teszt elvégzésével.

#015
Érdekmérlegelési teszt, segítség!

Az érdekmérlegelési teszt – első olvasásra elrettentő kifejezés –, az alábbiakat jelenti: ezzel állapítható meg, hogy az adatkezelés célja jogszerű-e (jogszerűség-vizsgálat). Ha igen, a következő lépésben azt kell megállapítani, hogy tényleg szükség van-e az adatkezelésre a cél eléréséhez (szükségesség-vizsgálat). Ha jelentős anyagi ráfordítás nélkül is elérhető a célunk az adatkezelés nélkül, akkor természetesen nem szükséges az adatkezelés, tehát jogos érdekekre hivatkozva már nem jogszerű az adatkezelés. Ám ha jogszerű az adatkezelés célja, és az ehhez szükséges adatkezelés is, meg kell vizsgálni, hogy a jogi érdekünk milyen arányban áll a személyes adat védelméhez kapcsolódó joggal (arányosság-vizsgálat).

A fenti vizsgálatok sok-sok kérdéssel és azok kiértékelésével hajthatóak végre. Ennek ellenére igen valószínű, hogy ez az egyik legnépszerűbb jogalap, ezért érdemes tájékozódnunk ennek részletszabályozásáról is, illetve megismerkedni és barátkozni a gyakorlati alkalmazásával.

#016
Mit is takarnak a hangzatos adatvédelmi elvek?

Az adatkezeléssel és adatvédelemmel kapcsolatban a GDPR-ban lefektetett elveknek akkor van igazán értelmük, ha a valóságban is megjelennek az adatkezelés teljes folyamatában, és az adatkezelők annak minden szakaszában betartják őket. Az alábbiakban a száraz és hosszú definíciók helyett rövid megfogalmazásokkal és gyakorlati példákkal szemléltetjük az adatvédelmi alapelvek jelentőségét:

01
Jogszerűség, tisztességes eljárás és átláthatóság elve

A személyes adatok kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni.

Adott egy weboldal, ahonnan termékeket vásárolok és megadom a személyes adataimat → ebben az esetben az adatkezelés teljesen jogszerű, hiszen én adtam meg az adatokat.

Értékesítőként dolgozom egy cégnél, ám a korábbi kollégám telefonjában tárolt természetes személyeket én már jogszerűen nem hívhatom fel → hiszen nincs megfelelő jogalapom rá, így az adatkezelés is jogszerűtlen lenne. Érdekes lehet ennek a fordítottja: magánszemélyként céges kontaktokat viszont nyugodt szívvel hívhatok, hiszen ez nem tartozik a GDPR hatálya alá. Ez persze felvethet további kérdéseket, mint például üzleti titok sérelme, etikai problémák, azonban ezek a kérdések már nem tartoznak az adatvédelem körébe.

02
Célhoz kötöttség elve:

A személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történjen, azokat ne kezeljék ezekkel a célokkal össze nem egyeztethető módon.

Egy rendezvényen résztvevők közötti sorsolás alapvetően kétféleképp is megvalósítható: a játékosok nevét és címét tartalmazó részvételi lapokat sorsolják ki, és a nyertes nevét bemondják, vagy pedig sorszámozott tombolaszelvényeket osztanak ki a résztvevők között, és a kihúzott sorszámmal megegyező tombola birtokosa nyer. Mivel a másodikként leírt eljárás is tökéletesen alkalmas az adott cél elérésére, az elsőként vázolt eset nem lesz jogszerű, ott feleslegesen kezelik sok száz ember adatait.

03
Adattakarékosság / adatminimalizálás elve:

A személyes adatoknak az adatkezelés céljai szempontjából megfelelőnek és relevánsnak kell lenniük, továbbá a szükséges mértékre kell korlátozódniuk. Nem lehet „készletre” dolgozni, csak a lehető legkevesebb adatot szabad begyűjteni.

Nem kérhető be a teljes születési dátum, ha csupán annyit szükséges tudnunk a weboldalunk felhasználójáról, hogy elmúlt-e 18 éves. Ugyanígy indokolatlan a pontos születési dátum kezelése, ha felhasználóinknak csupán születésnapi üdvözletet kívánunk küldeni, hiszen itt elegendő a hónap és nap ismerete is.

04
Korlátozott tárolhatóság:

A személyes adatokat olyan formában kell tárolni, amely az érintettek azonosítását csak az adatkezelés céljainak eléréséhez szükséges ideig teszi lehetővé.

Általánosságban elmondható, hogy a korlátlan ideig történő adatkezelés tiltott. Van, hogy jogszabály írja elő, meddig kell és lehet adatokat kezelni, például a számviteli bizonylatok esetében a számviteli törvény határozza meg a 8 éves határidőt. De ha nincs ilyen jogszabály, az adatkezelőnek kell azt meghatároznia. Mindig – szintén már az adatkezelés megkezdése előtt – meg kell határozni egy olyan határidőt, amelynek eltelte után az adatokat törölni fogjuk.

Például egy állásportál esetében, ha az álláskereső felhasználó már fél éve nem lépett be, akkor valószínű, hogy már talált állást, de ha nem, ilyen aktivitással nem is fog. Így sem a felhasználónak, sem pedig az állásportálnak nem érdeke, hogy a portál a felhasználó adatait tovább kezelje. Előzetes értesítés után az adatok törölhetők, sőt azokat törölni kell.

05
Pontosság elve:

A személyes adatoknak pontosnak, szükség esetén naprakésznek kell lenniük, és minden észszerű intézkedést meg kell tenni az adatkezelés céljai szempontjából pontatlan személyes adatok haladéktalan törlése vagy helyesbítése érdekében.

Ha valaki hitelszerződést akar kötni, a bank általában ellenőrzi a leendő ügyfél hitelképességét. E célból elérhetők speciális adatbankok (KHR-rendszer – régebben BAR-lista), amelyek magánszemélyek hiteltörténetére vonatkozóan tartalmaznak adatokat. Ha egy ilyen adatbázis helytelen vagy idejétmúlt adatokat tartalmaz valakiről, ez negatív hatással lehet az illetőre. Ezért az ilyen adatbázisok kezelőinek különösen törekedniük kell a pontosságra.

06
Integritás és bizalmas jelleg / adatbiztonság:

A személyes adatokat oly módon kell tárolni, hogy védve legyenek jogosulatlan vagy jogellenes kezeléstől, illetve ne lehessen elveszteni, megsemmisíteni vagy károsítani azokat.

Az integritás és bizalmi jelleg megőrzése lényegében az adatbiztonság gyakorlati megvalósításán keresztül történhet. Ehhez a fenti elvnek megfelelően kell megtervezni és kialakítani az egész adatkezelési folyamatot.

A védelem módját és mértékét mindig nekünk kell eldöntenünk a szervezetünk sajátosságait figyelembe véve – egy kétfős irodától nem várható el, hogy Fort Knox szintű védelmet biztosítson, ám az adatkezelő kötelessége, hogy minimum nehezen megfejthető jelszóval védje az adatbázisát, ne hagyja szanaszét a laptopját, legyen gyakran biztonsági mentés és az iratokat se vigye ki a huzat az ablakon.

Jó megoldás lehet az adatok álnevesítése, ami azt jelenti, hogy egy technikai vagy szervezési intézkedés keretében a személyes adatok – az érintett azonosítását lehetővé tevő – jellemzőit egy álnévre cserélik és elkülönítve tárolják. Az álnevesítést nem szabad összekeverni az anonimizálással, amelynél az egyént azonosító összes kapcsolatot megszüntetik.

#017

Hogyan állnak kapcsolatban az előbbi adatvédelmi elvek az elszámoltathatóság elvével?

Az adatkezelőkre vonatkozó elszámoltathatóság bevezetése a GDPR nagy újítása. Az adatkezelő köteles megfelelni a fentebb részletezett alapelveknek, és megfelelőségét dokumentumokkal alátámasztani. Tehát itt fordított bizonyítási kényszer áll fenn, azaz nem az adatvédelmi hatóságnak, üzleti partnernek, érintettnek kell bizonyítania, hogy jogszerűtlen kezelés történt, hanem a vállalkozásoknak kell az egyes adatkezelésükről dokumentumot vezetni, amelyet kérésre kötelesek az adatvédelmi hatóság vagy a bíróság részére átadni. Így bizonyítja a vállalkozás az adatvédelmi megfelelést.

A hatóságok külön figyelmet fordítanak az adatkezelés jogalapjára és céljára, valamint a címzettek körére, illetve az alkalmazott védelmi (technikai és szervezési) intézkedésekre. Az elszámolhatóság elve a gyakorlatban úgy teljesül, hogy egy aktában átnyújtjuk az ügyfelek, adatvédelmi hatóság és az érintettek részére mindazon jegyzőkönyvet, nyilvántartást és egyéb dokumentumokat, amelyek bizonyítják jogszerű eljárásunkat.

#018

Milyen jogaim vannak nekem mint érintettnek?

Milyen érintetti jogosítványokat tartsak szem előtt, ha adatkezelő vagyok?

A GDPR értelmezésében az érintett fogalma az azonosított vagy azonosítható természetes személyt jelöli, akinek személyes adatait az adatkezelő kezeli. Az érintetti jogok alapos ismerete iránymutatást ad az adatkezelés során arról, mi az, amit mindkét oldalon – érintettként és adatkezelőként is – szükséges szem előtt tartanunk. Fontos, hogy érintettként megfelelő ismeretekkel rendelkezzünk a minket érintő adatkezelésekről és kellően fel legyünk vértezve a személyes adatainkkal való esetleges visszaélésekre.

Adatkezelőként pedig maximálisan biztosítanunk kell az adatkezelési műveletek végzése során az érintettek számára az őket megillető jogok gyakorlását.

01
Tájékoztatáshoz való jog

A természetes személy jogosult személyes adatáról átlátható, tömör, könnyen fellelhető és egyszerű nyelvezetű tájékoztatást kapni az adatkezelés lényeges szempontjairól: ki, mit, mire, hogyan, mettől meddig használ, stb. – a GDPR pontosan meghatározza a szükséges információk körét.

A tájékoztatásnak lehetőleg már a személyes adatok felvétele előtt meg kell történnie. Ha erre nincs mód – mert például az adatokat harmadik személytől szerzik be – valaki elküldi egy barátja önéletrajzát a HR-osztálynak – úgy az első lehetséges időpontban.

02
Hozzáféréshez való jog

Ennek a jognak az újdonsága abban áll, hogy az érintettnek nem csak arra van joga, hogy tájékozódjon, milyen adatokat kezelnek róla, hanem arra is, hogy elkérje a személyes adatot tartalmazó adathordozót és annak másolatát.

Az adatkezelő köteles másolatot készíteni a személyes adatokról az érintett számára, például videofelvétel, feljegyzés formájában. Ezt köteles ingyenesen rendelkezésére bocsátani. Ha az érintett további másolatokat kíván igénybe venni, az adatkezelő az adminisztratív költségekért észszerű mértékű díjat számíthat fel.

Ha elektronikusan történik az adatigénylés, az adatkezelő széles körben használt formátumban bocsáthatja rendelkezésre az információkat. Ügyelni kell mindeközben arra, hogy a másokra vonatkozó információkat hozzáférhetetlenné kell tenni.

03
Helyesbítéshez való jog

Az érintett jelezheti, hogy a kezelt személyes adatai pontatlanok és kérheti, hogy azok helyett mit tüntessenek fel az adatbázisban. Az adatkezelőnek pedig indokolatlan késedelem nélkül korrigálnia kell az érintettre vonatkozó személyes adatokat.

04
Töréshez való jog

A GDPR kifejezetten előírja, hogy az érintett bármikor kérheti adatai törlését. Ha az adatkezelő hozzáférést engedett harmadik félnek a törölni kért adatokhoz, akkor fel kell szólítania mindazokat, akik számára nyilvánosságra hozta az érintett adatot, hogy minden hivatkozást, illetve náluk tárolt személyes adatot töröljenek. Ennek célja, hogy – hacsak annak jogi vagy észszerű akadálya nincs – az érintett adat „tűnjön el” a fellelhető adatbázisokból.

Törlésre adhat továbbá okot az is, ha megszűnt az adatkezelés célja, ha az érintett a hozzájárulását visszavonja, ha jogellenesen kezelték az adatokat, illetve ha az érintett tiltakozik az adatkezelés ellen.

05
Tiltakozáshoz való jog

Az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból kifolyólag bármikor tiltakozzon személyes adatainak kezelése ellen. Ez tipikusan akkor szokott megtörténni, amikor az érintett nem adta hozzájárulását személyes adatai adott kezeléséhez. Ezzel összefüggésben elsősorban a jogos érdeken alapuló adatkezeléshez kapcsolódóan biztosít jogot az érintett részére. Tiltakozás esetén az adatkezelő a személyes adatokat nem kezelheti tovább, kivéve, ha bizonyítja, hogy az adatkezelést olyan kényszerítő erejű jogos okok indokolják, amelyek elsőbbséget élveznek az érintett érdekeivel, jogaival és szabadságaival szemben, vagy amelyek jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódnak.

A Manni ügyben az Európai Bíróság megállapította, hogy a személyes adatok cégnyilvántartásban való közzétételének törvényes célja és a harmadik személyek érdekei védelmének szükségessége miatt S. Manni nem jogosult személyes adatainak törlését kérni a cégnyilvántartásból.[2] A bíróság tisztázta, hogy Manni esetében kizárólag azon körülmény, miszerint potenciális ügyfélkörét állítólag befolyásolta személyes adatainak közzététele, nem minősül jogos és kényszerítő oknak.[2] Manni potenciális ügyfeleinek jogos érdekük fűződik a régi vállalkozásának csődjére vonatkozó információkat megismerni.[2]

[2]Forrás: https://curia.europa.eu/jcms/upload/docs/application/pdf/2017-03/cp170027hu.pdf

06
Automatizált adatkezelés

Korábban a profilalkotáshoz kapcsolódóan említettük az automatizált adatkezelést. Az érintetti jogok tükrében fontos kiemelni, hogy az érintettnek joga van arra, hogy rá ne terjedjen ki a kizárólag automatizált adatkezeléssel történő döntés hatálya.

#019
Mit kell tudnunk az adatvédelmi incidensekről?

A fogalom két kulcselemre bontható: egyrészt az adatvédelmi incidens mindenképpen egy biztonsági eseményre kell, hogy visszavezethető legyen, másrészt ebből a biztonsági sérülésből kell majd következnie egy jogellenes vagy véletlen személyesadat-közlésnek, vagy adott esetben megsemmisülésnek, elvesztésnek, jogosulatlan hozzáférésnek.

#020
Megelőzhető az adatvédelmi incidens?

Az adatkezelők és adatfeldolgozók felelőssége, hogy lehetőleg mindent megtegyenek a személyes adatok biztonságos kezelése érdekében, de egy adatvédelmi incidens ettől függetlenül, akár közel tökéletes biztonsági intézkedések mellett is bekövetkezhet.

Gyakori példa egy külső hackertámadás bekövetkezése; például egy jelentősebb adatmennyiséget kezelő egészségügyi szolgáltató rendszerében sérülékenység érzékelhető, amelyet egy hacker felfedez, így a páciensek különleges adatai könnyen eshetnek a jogosulatlan hozzáférés áldozatául – az adatvédelmi incidens máris bekövetkezett.

#021
Mit tehetek érintettként, ha adatvédelmi incidens során kerülnek illetéktelen kézbe a személyes adataim?

A jogsértések érintetti észlelése elég gyakori. Ezekben az esetekben az érintett megfelelően valószínűsíteni tudja, hogy mely adatkezelőtől kerülhettek ki az adatai. Ilyen esetekben egyrészt jelezheti az aggályát az adatkezelőnek, ekkor az adatkezelő GDPR-ból eredő kötelezettsége az érintett tájékoztatása arra vonatkozóan, hogy bármilyen adatvédelmi incidens keretében sérült-e személyes adatai biztonsága. A másik lehetősége, hogy közvetlenül az adatvédelmi hatósághoz fordul.

A tapasztalat azt mutatja, hogy viszonylag sok az olyan érintetti bejelentés, amelyben nem sérült a biztonság és nem szivárogtak ki személyes adatok, „csupán” a nem kis számban elterjedt csaló-levelekben előadottak keltettek félelmet az érintettben. Az ilyen csaló-levelekben a feladó által előadott történetek (pl. laptopfeltörés, lefilmezés) legtöbbször nem igazak, csupán a félelemkeltést és azt célozzák, hogy a címzettől minél több pénzt csikarhassanak ki személyes adataira hivatkozva.

Arra is volt már példa, hogy elegendő bizonyítékot nyújtott be az érintett, amelyekkel alátámasztotta, hogy a csalás során jelentős anyagi kár is érte, ilyen esetekben átkerül az ügy a nyomozó hatósághoz, mivel bűncselekmény gyanúja esetén már az jogosult az ügyben eljárni.

#022
Ki az az adatvédelmi tisztviselő, és mi a feladata?

Az adatvédelmi tisztviselő nem a GDPR újítása, már korábban is ismert volt az úgynevezett adatvédelmi biztos személyében. A GDPR hatálybalépését követően lett az elnevezése a ma is használt adatvédelmi tisztviselő. Akit nem feltétlenül kell kinevezni, csak a GDPR-ban meghatározott esetekben, vagyis közhatalmi szerveknél, az adatalanyok nagymértékű megfigyelése esetén (pl. vagyonvédelem), illetve különleges személyes adatok kezelése esetén (pl. kórház). Az adatvédelmi tisztviselő egyébként lehet alkalmazott vagy külső megbízott is.

E felkészült adatvédelmi szakember tájékoztat, szakmai tanácsot ad a GDPR-rendelettel kapcsolatban, ellenőrzi a betartását, belső szabályok elkészítésével és megfelelésével kapcsolatos teendőket végez, hozzájárul az adatvédelmi tudatosság növeléséhez, együttműködik a felügyeleti hatósággal, illetve kapcsolattartóként is szolgál.

#023
Nem félünk a farkastól!? — avagy milyen hatóság a NAIH és kell-e tőle tartani?

A NAIH, azaz a Nemzeti Adatvédelmi és Információszabadság Hatóság a személyes adatok védelméért felelős független magyar szervezet, feladata a személyes adatok védelméhez való jog érvényesülésének ellenőrzése és elősegítése. Magyarországon a NAIH felel végső soron a GDPR betartatásáért, ellenőrzéseket folytathat le, az adatvédelmi szabályok megsértőit szankcionálhatja. Emellett iránymutató, jogszabály -értelmezést segítő, továbbá nemzetközi vonatkozású feladatai is vannak.

A NAIH oldalán (www.naih.hu) számtalan állásfoglalás, ajánlás, jogeset, határozat, oktatási segédanyag, magyarázat található. A NAIH kiemelt figyelmet fordít az érdeklődők folyamatos tájékoztatására, informálására, érdemes böngészni az oldalukat, hogy átfogó képet kapjunk az adatvédelem mibenlétéről, szabályozásáról. Ezek a segédanyagok azonban nem csupán tájékoztatási, hanem „kvázi jogforrási”, angol terminológiával élve „soft law” jelleggel is bírnak.

Az adatvédelmi hatóságnak kezdetben inkább tanító, nevelő, iránymutató, értelmezést segítő tevékenysége volt a számottevő, ám napjainkra szankcionáló funkciója is erőteljesen előtérbe került. Ez bizony azt is jelenti, hogy a NAIH bírságol a GDPR megsértése miatt.

#024

Mi történik, ha nem tartom be a GDPR előírásait?

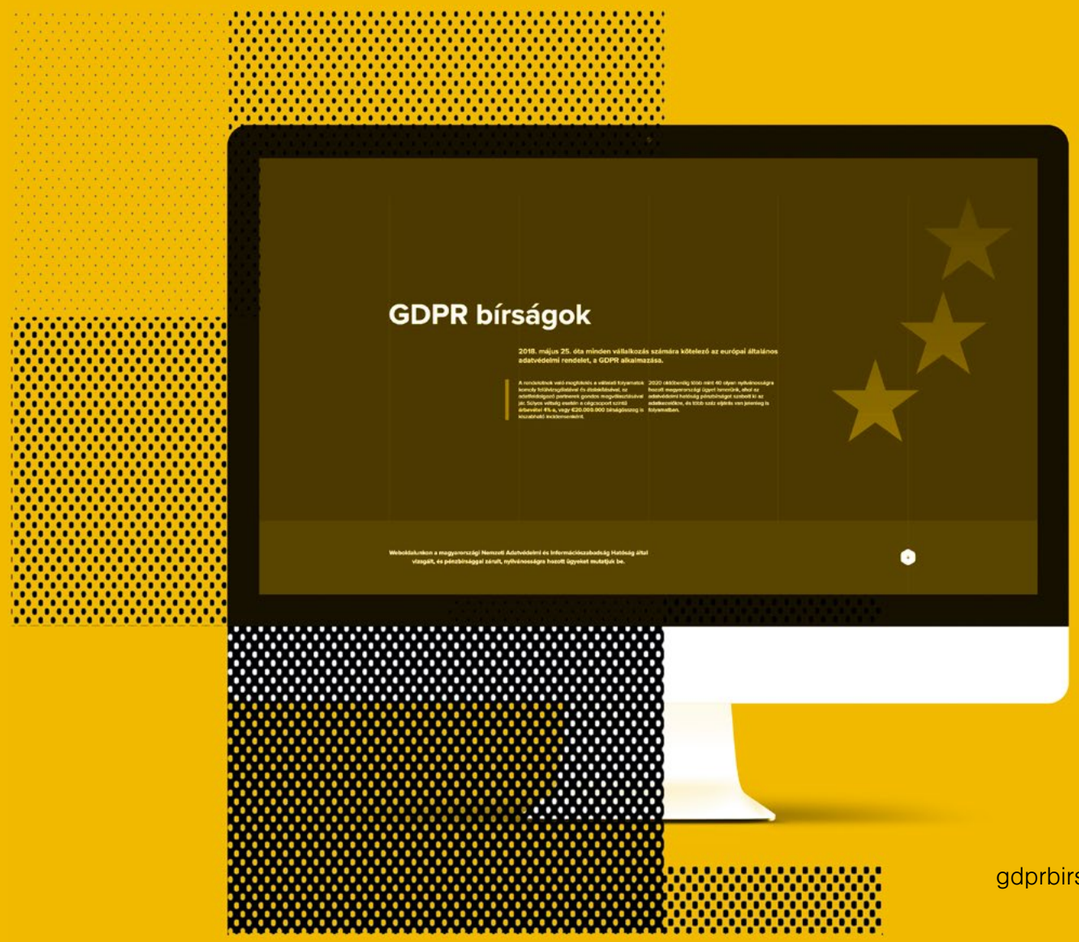
A fenti pontban rögzítettek szerint nagy eséllyel számolhatunk azzal, hogy akár egy névtelen bejelentéssel, akár hivatalból megindult eljárás szenvedő alanyává válunk, ha nem fordítunk kellő figyelmet az adatvédelmi szabályok betartására, az érintetteket illető jogok maximális betartására, esetleg nem vagyunk együttműködőek egy már megtörtént adatvédelmi jogsértést követően.

A NAIH vizsgálati eljárás vagy hatósági eljárás lefolytatásával járhat el. A hatósági eljárás egyik következménye lehet a közigazgatási bírság kiszabása. Az adatvédelmi bírság maximális mértéke a jogsértés jellegétől és az összes körülménytől függően:

01 *10 millió euró, illetve vállalkozások esetében az előző pénzügyi év teljes éves világpiaci forgalmának 2 %-a – a kettő közül a magasabb összeget kell kiszabni,*

02 *20 millió euró, illetve vállalkozások esetében az előző pénzügyi év teljes éves világpiaci forgalmának 4 %-a – a kettő közül a magasabb összeget kell kiszabni.*

A tagállamoknak jogukban áll adatvédelmi jogsértések esetén további büntetőjogi szankciókat kiszabni.



Tudnunk kell azonban, hogy az adatvédelmi hatóságnak nem a bírságolás az egyetlen eszköze: az Infotörvény alapján felszólítást intézhet a jogsértő adatkezelő irányába a jogsérelem orvoslására, illetve annak közvetlen veszélye megszüntetésére. Más esetekben – felügyeleti szervvel rendelkező adatkezelő hatóságnál – pedig ajánlást tehet az adatkezelő felügyeleti szervnek.

#025

GDPR kontra hazai jogszabályok – most akkor melyiket kell alkalmazni?

Ahogyan arról a korábbiakban szóltunk, a GDPR nem igényel, de még csak nem is tűr nemzeti átültetést: a rendeletben foglaltakat a tagállamok saját jogszabályaikban nem ismételhetik meg, önálló szabályozást a GDPR hatálya alá tartozó adatkezelésekre pedig csak akkor alkothatnak vagy tarthatnak fenn, ha azt maga a GDPR megengedi. A rendelet összesen ötvennél több kérdésben enged teret a tagállami jogalkotásnak.

A GDPR közvetlen hatályából és az uniós jog nemzeti joggal szembeni alkalmazási elsőbbségéből következik, hogy a GDPR által megengedett kivételeken és eltéréseken túlterjeszkedő, mindenkor hatályban lévő magyar szabályokat nem, illetve azok helyett a GDPR szabályait kell alkalmazni.

Fentiek szerint, optimális esetben, illetve ha bízhatunk a jogalkotókban, akkor napjainkban már nincs, legalábbis nem kellene lennie olyan magyar jogszabálynak, amely rendeleti megengedés, felhatalmazás nélkül szabályoz adatvédelmi kérdéseket. Ha mégis találunk ilyet, azok helyett is a rendeletet kell alkalmazni.

Mindezeknek megfelelően az Infotörvény alkalmazása során kiemelt figyelmet kell fordítani arra, hogy a rendelet hatálya alá tartozó adatkezelések esetén kizárólag azon előírásai alkalmazandók, amelyeket ő maga a rendeletet kiegészítő normaként alkalmazni rendel. Az Infotv. minden további rendelkezését a rendelet hatálya alá tartozó jogviszonyokban nem kell és – a vonatkozó uniós jog jellegére és tartalmára figyelemmel – nem is lehet alkalmazni.

A kiadványunk első részében foglalt hasznos információk átböngészését követően egy kicsit közelebb kerülhettünk az adatvédelmi szabályozás rendszeréhez, alapjaihoz, fontosabb fogalmaihoz, kifejezéseihez. Talán már nem is lesz olyan idegen jobban belemélyülni a szabályozás speciálisabb, részletesebb leírásába, ami számos izgalmas kérdést tartogat még.

A következő részben érintjük a kis- és középvállalkozások, valamint az egyéni vállalkozók helyzetét, továbbá elkalauzoljuk az Olvasókat a munkahelyi adatkezelés világába, sőt, a hírlevelek, a direkt marketing és cookie-k frontján is tartogatunk hasznos információkat.

crosssec.com

tanacsadas.crosssec.com

crosssec
solutions

crosssec.com
tanacsadas.crosssec.com