HOLLÓ VAS & FÜLÖP
ÜGYVÉDI TÁRSULÁS

Adatvédelem

„A gyors technológiai fejlődés és a globalizáció új kihívások elé állította a személyes adatok védelmét. A technológia a vállalkozások és a közhatalmi szervek számára tevékenységük folytatásához a személyes adatok felhasználását minden eddiginél nagyobb mértékben lehetővé teszi. Az emberek egyre nagyobb mértékben hoznak nyilvánosságra és tesznek globális szinten elérhetővé személyes adatokat. A technológia egyaránt átalakította a gazdasági és a társadalmi életet, és egyre inkább elősegíti a személyes adatok [...] szabad áramlását [...]”

– az általános adatvédelmi rendelet, közismert nevén „GDPR” (6) preambulumbekezdése

CÉLOK ÉS FEJLŐDÉSI TENDENCIÁK

Privát szféra védelme

A GDPR megalkotóinak célja, hogy a technológiai fejlődés személyes adatok szabad áramlásával összefüggő szabályozására szilárd alapokat és szankciókat kínáljon.

„A természetes személyek számára biztosítani kell, hogy saját személyes adataik felett maguk rendelkezzenek. A természetes személyek, a gazdasági szereplők és a közhatalmi szervek számára a jogbiztonságot és a gyakorlati biztonságot fokozni kell."

– GDPR (7) preambulumbekezdése

A személyes adatok védelme alapvető jog, amit az Európai Unió Alapjogi Chartája a következőképpen szabályoz:
„Az ilyen adatokat csak tisztességesen és jóhiszeműen, meghatározott célokra, az érintett személy hozzájárulása alapján vagy valamilyen más, a törvényben rögzített jogos okból lehet kezelni. Mindenkinek joga van ahhoz, hogy a róla gyűjtött adatokat megismerje, és joga van azokat kijavíttatni."

A személyes adatok védelmének kapcsolata más alapvető jogokkal

A személyes adatok védelméhez való jogot az arányosság elvével összhangban, a társadalomban betöltött szerepének függvényében kell figyelembe venni, egyensúlyban más alapvető jogokkal, különösen a magán- és a családi élet, az otthon és a kapcsolattartás tiszteletben tartásához való alapvető joggal, továbbá a gondolat-, a lelkiismeret- és a vallásszabadsághoz, a véleménynyilvánítás szabadságához, a tájékozódás szabadságához, a vállalkozás szabadságához, a tisztességes eljáráshoz fűződő jogokkal, valamint a kulturális, vallási és nyelvi sokféleséghez való joggal.

Adatvédelem hazánkban

Magyarország a személyes adatok védelmére már a rendszerváltástól kiemelt hangsúlyt fordított. A személyes adatok védelmének európai összehasonlításban is magas szintjét biztosította az Alkotmány, a 1992. évi adatvédelmi törvény, illetve az ezek nyomán kialakult alkotmánybírósági gyakorlat. Ezt a szintet az Alaptörvény és az Infotv. nemcsak fenntartotta, hanem a személyes adatok védelméhez fűződő jog érvényesülésének ellenőrzésére és elősegítésére létrehozta a Nemzeti Adatvédelmi és Információszabadság Hatóságot („NAIH"). A személyes adatok védelmének hazánkban biztosított szintje az Európai Unió tagállamai között az egyik legmagasabbnak tekinthető.

Adatbiztonság

Az adatbiztonsági elvárások szerves részét képezik az adatvédelmi szabályozásnak, amit a GDPR az alapelvek szintjén is kifejez.

„A személyes adatok kezelését oly módon kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve."

– GDPR 5. cikk (1) bekezdés f) pont

A szabályozás technológiasemleges és szükség szerint rugalmas – a jogalkotó régóta ismert és elfogadott szabályokat és jó gyakorlatokat állít középpontba.

ADATSZIVÁRGÁS ELLENI VÉDELEM LÉPÉSEI

1. *Veszélyforrások feltérképezése*
2. *A védendő adatok és információk azonosítása és osztályozása*
3. *Adatvédelmi szabályozás kialakítása és folyamatok megtervezése*
4. *Automatizált technológiák bevezetése*
5. *Belső képzések, az adatvédelem integrálása az folyamatokba*
6. *Hosszú távú stratégiák kialakítása*

A kkv szektor felelőssége

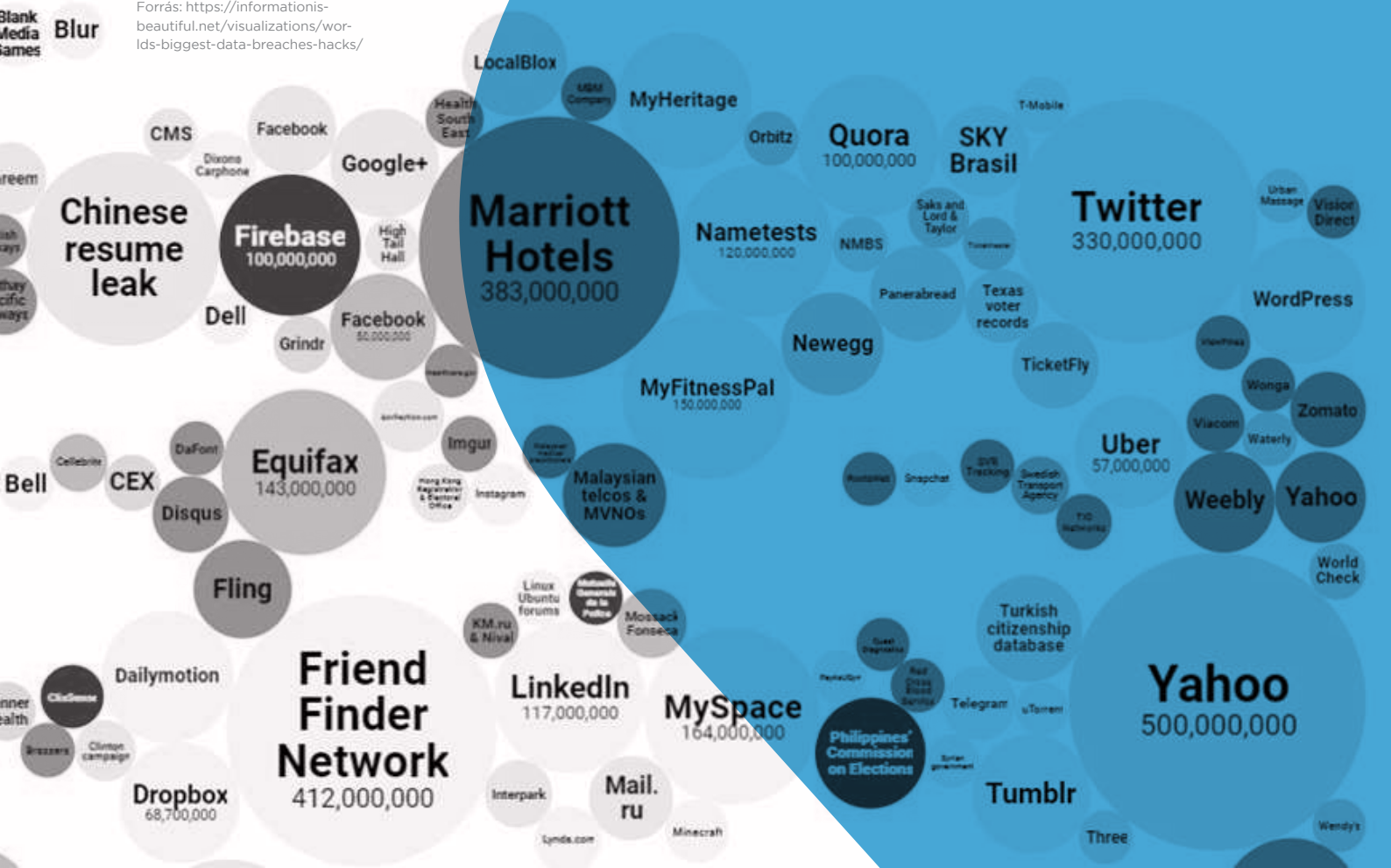
A kiberbűnözök a nagyobb cégekhez sokszor a kevésbé védett kis- és középvállalkozásokon keresztül jutnak el, akik közreműködőként, beszállítóként, egyéb üzleti partnerként hozzáférnek a célpont által kezelt személyes adatokhoz. Mindezek miatt fontos, hogy a kis- és középvállalkozások is kiemelt figyelmet fordítsanak az adatbiztonsági intézkedésekre a támadások megelőzése érdekében.

TIPP NAGYOBB CÉGEKNEK:

A vezetőik és az alkalmazottaik rendszeres oktatásán túl fordítsanak figyelmet a beszállítók oktatására is, továbbá használjanak titkosító megoldásokat a hordozható eszközök védelmére, és készítsenek rendszeresen biztonsági mentéseket.

Jelentősebb adatszivárgások a közelmúltban:

Forrás: https://informationis-beautiful.net/visualizations/worlds-biggest-data-breaches-hacks/



AZ ADATVÉDELMI MEGFELELÉS GYAKORLATI LÉPÉSEI

Az adatkezelő vezetője kulcsszereplő a közös célok meghatározása, a folyamat elindítása során, valamint abban, hogy olyan rendszert dolgozzon ki, melyben a kialakított jó gyakorlatok működni tudnak, a működés pedig időről-időre ellenőrizhető. A jogszerű működést több síkon kell biztosítani: egyrészt az adatvédelmi jogszabályok által meghatározott dokumentációs rend elkészítésével és folyamatos vezetésével, másrészt a dokumentumokban foglaltak betartásával. A megfelelésnek nincs „kulcsrakész" megoldása, a megfelelés nem vásárolható meg komplett csomagokban, hiszen minden cég működése egyedi, így egyedi adatvédelmi megoldásokat igényel.

Adatvagyon felmérése, adatleltár elkészítése

MIT

Az adatvédelmi megfelelés első lépése, hogy az adatkezelő felmérje a birtokában lévő adatokat, arról leltárt készítsen. Ennek keretében fel kell mérnie, hogy a szervezetén belül mely egységek, milyen személyes adatokat kezelnek akár papír alapon, akár elektronikusan, akár elszórtan, akár nyilvántartásba, adatbázisba rendezve; akik hozzáférnek az adatokhoz, nekik valóban hozzá kell-e férniük; végül a személyes adatok mely kategóriái fordulnak elő az adatkezelőnél, pl. kezelnek-e különleges személyes adatokat (egészségügyi adatokat, vallási vagy világnézeti meggyőződésre, szakszervezeti tagságra utaló személyes adatokat), esetleg minősített adatokat.

Adatkezelési gyakorlat vizsgálata: adattérkép

MIÉRT, HOGYAN

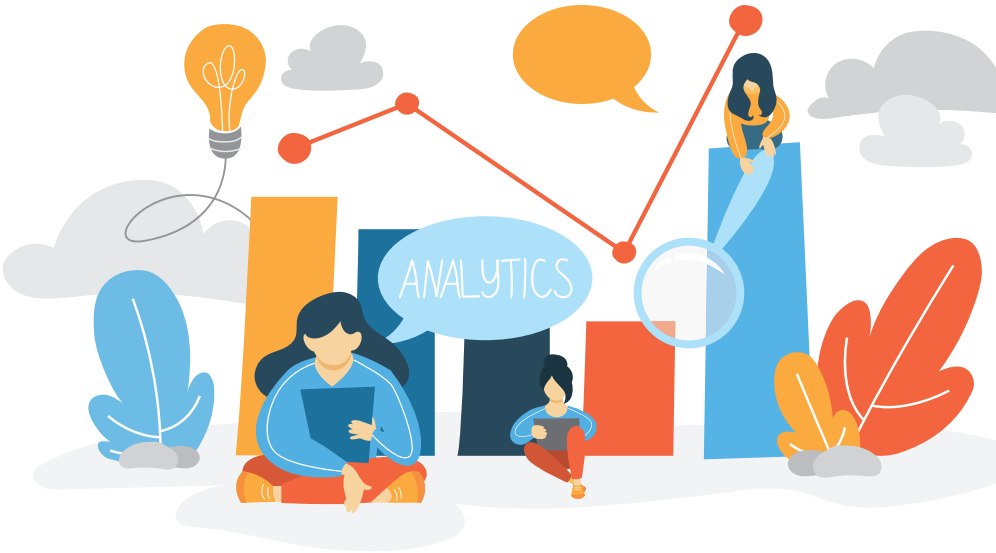
Az adatkezelő az adattérkép elkészítése során, az adatleltár alapján számba veszi, hogy a személyes adatait kezelő belső, külső személyek / szervezetek / szervek hogyan kezelik, tehát az adatáramlás útját (okát és célját) mérik fel. Ez akár vizuálisan is ábrázolható, illetve kiterjedhet valamennyi adatkezelésre, vagy esetlegesen részterületekre is. Az adattérkép elkészítése nemcsak a folyamatok átláthatóvá tételét segíti elő, de az adatkezelés egyes szereplőinek (érintettek, adatkezelők, adatfeldolgozók, más címzettek) az azonosítását is nagyban megkönnyíti.

A jogi szakértő szerepe

TEGYÜNK RENDET

Ha a személyes adatok körének azonosítása megtörtént, ezt követően kezdetét veheti az adatvédelmi megfelelés érdemi, szakmai része. A megfelelés szükségszerű aktív közreműködői az adatkezelő szervezeti egységeinek a vezetői (pl. HR, belső ellenőrzés, pénzügy, informatika), akik a hatáskörük szerinti folyamatokat részletesen és pontosan, a napi ügymenet szemszögéből is ismerik. Amennyiben szervezeten kívüli egység is kezel személyes adatokat (jellemzően a marketing és az informatika területe), ebben az esetben őket is be kell vonni.

A jogi szakértő bevonásával pedig kezdetét veheti az adatvédelmi jogi átvilágítás: az esetleges szabálytalanságok feltárása, kockázatok azonosítása, helyes gyakorlatok megalapozása.
Az adatvédelmi megfelelés jogi támogatását az adatvédelemben járatos, kellő tapasztalattal rendelkező jogi szakértőre érdemes bízni arra tekintettel, hogy az adatvédelmi joganyag alkalmazása nemcsak a GDPR és az Infotv. alapos ismertét feltételezi, hanem a hatályos más jogszabályok, ágazati rendelkezések, valamint a tagállami adatvédelmi hatóságok és az unió adatvédelmi konzultációs szerveinek a jogértelmezési gyakorlatának az ismeretét és folyamatos nyomon követését is.



TEGYÜNK RENDET

A szervezet szerepe

Az esetleges szabálytalanságok és kockázatok azonosítását követően a jogi szakértő előkészíti az adatvédelmi megfeleléshez szükséges dokumentumokat, melyek véglegesítésére az adatkezelő területi vezetőinek és egyéb felelősöknek az aktív közreműködésével kerül sor. A dokumentáció hasznosulása, a közös munka hatékonysága függ attól, hogy mennyire sikerül az adott szervezet sajátosságaihoz igazítani a dokumentációs rendet. Éppen ezért kiemelten fontos, hogy az adatvédelmi megfelelés koordinálására az adatkezelő a belső működését kellő mélységben ismerő személyt delegáljon, aki összehangolja a jogi szakértő, a területi vezetők munkáját és a vezetés elvárásait.

TARTSUK FENN A RENDET

Oktatás (jogi szakértő bevonásával)

A munkavállalók adatvédelmi oktatása és a megszerzett ismeretek ellenőrzése kiemelt fontosságú, hiszen az adatvédelmi megfelelés mit sem ér, ha a kialakított gyakorlatok és eljárások a papírformán túl nem lépnek ki a napi ügymenetet kezelő munkavállalók világába. A leggyakrabban előforduló, legtriviálisabbnak tűnő adatvédelmi kockázatok az emberi tényezőre vezethetőek vissza. Elég, ha az egyszeri munkavállaló a céges eszközén olyan fertőzött elektronikus levelet nyit meg, mely egy zsarolóvírust aktiválva akár évekre visszamenőleg zárolja, rosszabb esetben le is másolja az adatkezelő valamennyi adatát, ezzel súlyos adatvédelmi incidenst előidézve.

Kit nevezzünk ki adatvédelmi tisztviselőnek?

A GDPR bizonyos adatkezelők és adatfeldolgozók esetében kötelezővé teszi adatvédelmi tisztviselő kijelölését. Amennyiben a GDPR kötelezővé teszi, ennek elmulasztása önálló szankciót von maga után, még akkor is, ha az adatkezelő minden adatkezelést jogszerűen végez.
Az adatvédelmi tisztviselő minden esetben az adatvédelmi megfelelőséget kell, hogy szolgálja, néha az adatkezelő utasításaival és gazdasági érdekeivel szemben is. Az adatvédelmi tisztviselőt szakmai rátermettség és különösen az adatvédelmi jog és gyakorlat szakértői szintű ismerete és az adatvédelmi tisztviselői feladatok ellátására való alkalmasság alapján kell kijelölni.

HA ADATVÉDELMI TISZTVISELŐT JELÖLÖK KI, ÁTHÁRÍTHATOM RÁ A FELELŐSSÉGET?

Nem. Az adatvédelmi tisztviselő tanácsadási, ellenőrzési, együttműködési és egyéb feladatai körében a tevékenységéért felelősséggel tartozik ugyan, nem terheli azonban személyes felelősség az adatvédelmi megfelelőségért. Kizárólag az adatkezelő és az adatfeldolgozó felelős az adatvédelmi rendelkezések betartásáért, a felelősség így nem hárítható az adatvédelmi tisztviselőre.

Az elmélet harmadik típusú találkozása a gyakorlattal

A személyes adatok jelenléte a hétköznapok mikro-szintjéig ható jelenség, az adatvédelmi jogszabályok pedig a lehető legszélesebb körben tartalmaznak kötelező előírást. A minden élethelyzetre kiterjedő szabályozás azonban egyrészt lehetetlen, másrészt nem is kívánatos. Ezen ellentmondás ugyanakkor felveti annak a kérdését, hogy lehetséges-e a teljeskörű adatvédelmi jogi megfelelés. A jelen kiadvány közreadása idején adható válasz szerint nem. Gondolhatunk itt akár a személyes adatok törlésére vonatkozó szabályok gyakorlati, informatikai megvalósítására, mely jelenleg az IT szakemberek számára is egy megoldandó nyitott kérdés. Az adatkezelő a megfelelés kérdésére így tekinthet úgy is, mint a kockázatmenedzsment egy lehetséges területére, és ennek megfelelően szükséges teljesítenie a jogszabályi előírásokat.

ADATVÉDELEM SPECIÁLIS ÉS HANGSÚLYOS TERÜLETEI

1 Munkaügyi adatkezelés

A munkaügyi adatkezelésekben az egyik speciális elem a jogalap kérdése. Alapvetően a munkaügyi jogszabályok vagy a munkáltató jogos érdeke szolgáltatnak megfelelő jogalapot az adatkezeléshez, azonban szűk körben az érintett (tehát a munkavállaló) hozzájárulása alapján lesz jogszerű az adatkezelés. A hozzájárulás GDPR által előírt feltételeit (különösen az önkéntességet) ilyenkor semmi esetre sem lehet kiterjesztően értelmezni, ugyanis az önkéntesség megkérdőjelezhető minden alá-fölérendeltségi viszonyban.

A munkaügyi adatkezelés körében kiemelendő még a munkavállalók ellenőrzésével kapcsolatos adatkezelés.

Bár a munka törvénykönyvének 11/A. §-a lehetőséget biztosít a munkáltatónak a munkavállaló ellenőrzésére, az ellenőrzés jogszabályi követelményeinek történő megfelelés azonban komoly gyakorlati problémák elé állítja a munkáltatót. Az ellenőrzés megkezdése előtt minden esetben egy ún. érdekmérlegelési tesztet kell elvégeznie a munkáltatónak.

2 Gyermekek adatainak kezelése

A gyermekek az adatvédelmi jog szabályrendszerében is különös védelmet élveznek arra tekintettel, hogy ők kevésbé lehetnek tisztában a személyes adatok kezelésével összefüggő kockázatokkal, és azok következményeivel.

MIKOR DÖNTHET A GYERMEK ÖNÁLLÓAN SZEMÉLYES ADATAI SORSÁRÓL?

A GDPR szerint a közvetlenül gyermekeknek kínált, információs társadalommal összefüggő szolgáltatások vonatkozásában végzett személyes adatok kezelése akkor jogszerű, ha a gyermek a 16. életévét betöltötte, és a gyermek hozzájárulásának megadását a tervezett adatkezelés vonatkozásában megfelelő tájékoztatás (tömör, átlátható, gyermek számára érthető) előzte meg. A 16. életévét be nem töltött gyermek esetén a hozzájárulást jogszerűen a gyermek feletti szülői felügyeletet gyakorló adhatja meg. Az egyéb típusú adatkezelések vonatkozásában sem a GDPR, sem a jelenleg hatályos Infotv. nem tartalmaz külön rendelkezést.

Az adatkezelőnek különös körültekintéssel kell eljárnia és érdekmérlegelési tesztet kell elvégeznie, ha az adatkezelése jogalapjaként a jogos érdeket kívánja alkalmazni és az adatkezeléssel érintettek gyermekek.

3 Webáruházak

A honlap beállításaitól függően rengeteg adat azonosítható a honlap látogatójáról, pl. a látogató IP címe, a látogató honnan, mikor érkezett a honlapra, a honlapon mit tekintette meg, a látogató szokásaira vonatkozó következtetések is levonhatóak, melyeknek megfelelő célzott ajánlatok címzettje lehet anélkül, hogy egyáltalán elkezdett volna vásárolni. A vásárlással szükségszerűen együtt járnak további adatkezelések is: a webáruház üzemeltetője egészen biztosan kezelni fogja az online megrendelés teljesítéséhez adatokat (számlázáshoz, kiszállításhoz szükséges személyes adatok). Az adatkezelőt az adatvédelmi jogszabályok rendelkezései szerint kiterjedt tájékoztatási kötelezettség terheli, illetve köteles beszerezni az érintett esetlegesen szükséges hozzájáruló nyilatkozatát.

A webáruházak jogszerű működtetése természetesen jóval túlmutat az itt vázolt általános szabályokon, de az adatvédelmi jog területén is: a gyakorlat átvezet az elektronikus kereskedelem jogának területére, a reklámjog, a fogyasztóvédelmi jog, domain jog, szerzői jog, védjegyjog stb. szabályainak szintéziseként létezik.

4 Online direkt marketing

Az online közeg adta lehetőségek okos használata a digitális korral lépést tartó vállalkozásokat behozhatatlan versenyelőnyhöz juttathatja, hiszen egyrészt új és globális szintű értékesítési csatornákat nyit meg számukra, másrészt az egyes célcsoportokat célzott, személyre szabott ajánlatokkal kereshetik fel. Az online direkt marketing tipikus esete a hírlevélküldés, illetve a targetált reklámok megjelenítése. A vállalkozások ezen tevékenységük folytatása során szükségszerűen kezelnek személyes adatnak minősülő adatot is. A jelenlegi hazai és uniós szabályozási környezetben ezt úgynevezett „opt-in” módon, tehát az érintett előzetesen, egyértelműen és kifejezetten megtett hozzájárulásával tehetik meg. A hozzájárulás megadása a gyakorlatban leggyakrabban a nyilatkozat megtételére vonatkozó üres „check-box” kipipálását jelenti. Mivel a hozzájárulás megadása körében a GDPR tevőleges magatartást vár el, nem elfogadható az a gyakorlat, ha a vállalkozás előre kipipált „check-box”-ot alkalmaz. A sütik (cookie-k), mint lehetséges online direkt marketing eszközök használatának jogszerűsége hasonlóan biztosítható (ld. lentebb).

5 Kamerás megfigyelés

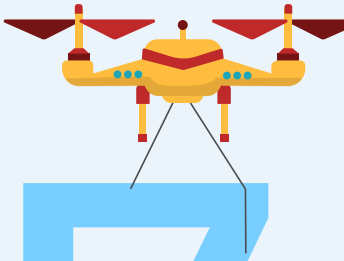
A GDPR salátatörvény alapjaiban írja újra a személy és vagyonvédelmi célból alkalmazott kamerarendszerre vonatkozó szabályokat. Egyrészt kezeli az alkalmazható jogalapok tekintetében fennálló korábbi szabályozási töredezettséget, tehát mind a munkavállalók, mind más személyek vonatkozásában is egységesen az adatkezelő vagy harmadik fél jogos érdeke biztosítja az adatkezelés jogszerűségét. Megjegyzendő, hogy munkavállalókat (is) rögzítő felvételek esetében a felek alá-fölérendeltsége okán a hozzájárulás mint jogalap vonatkozásában az önkéntesség eddig sem volt értelmezhető a NAIH gyakorlatában. Másrészt a GDPR salátatörvény a kamerafelvételek őrzési idejében is hoz nóvumot, az adatkezelő gyakorlatához rugalmasan igazodva a felvételek őrzési idejének meghatározását szintén az adatkezelő jogos érdekén belüli mérlegelés tárgyává teszi.

Mint minden más adatkezelés során, az adatkezelőt előzetes tájékoztatási kötelezettség terheli az adatkezelés jogszabályban meghatározott feltételeiről, továbbá a megfigyelt területre belépő személy figyelmét piktogrammal is fel kell hívni a kamera-rendszer alkalmazásának tényére.

6 Biometrikus adatok kezelése

A biometrikus adatok az ember abszolút értelemben vett, kétséget kizáró azonosítására alkalmas adatok, kezelésükre is kizárólag ezen célból kerülhet sor. A biometrikus adatok érzékenységét mutatja, hogy a GDPR a személyes adatok különleges kategóriái között helyezte el. Ezen adatok kezelése főszabály szerint tilos, a GDPR 9. cikkének (2) bekezdése tartalmazza azokat a kivételszabályokat, melyek mentén - ha a GDPR 6. cikkében felsorolt megfelelő jogalap is az adatkezelő rendelkezésére áll – jogszerű lehet a biometrikus adatok kezelése. A GDPR a biometrikus adatok körében példálózóan említi az arcképet vagy a daktiloszkópiai adatot, de az érintett egyedi azonosítására többek között retina vagy vénamintázata, DNS-e, aláírása, jellegzetes járása, viselkedése, hangja alapján is sor kerülhet.

A GDPR salátatörvény nyomán a Munka törvénykönyve kiegészül a munkavállaló biometrikus adatainak kezelésére vonatkozó szabályokkal: a munkavállaló biometrikus adata az érintett azonosítása céljából abban az esetben kezelhető, ha ez valamely dologhoz vagy adathoz történő olyan jogosulatlan hozzáférés megakadályozásához szükséges, amely 1) a munkavállaló vagy mások élete, testi épsége vagy egészsége, vagy 2) törvényben védett jelentős érdek súlyos vagy tömeges, visszafordíthatatlan sérelmének a veszélyével járna.



7 Drónok és adatvédelem

A drónok használata nem szükségszerűen, de jellemzően felvet bizonyos adatvédelmi kérdéseket. Ez alapvetően a drónokra szerelt eszközöknek köszönhető. Ezen eszközök lehetnek képfelvételre alkalmas kamerák, mozgásérzékelő szenzorok, rádió frekvenciás szenzorok és egyéb speciális szenzorok. A GDPR hatályát vizsgálva megállapítható, hogy az a drónok állami és kereskedelmi célú felhasználására terjed ki, ezzel szemben a magáncélú felhasználásra nem. A megfelelő szabályok hiánya a hazai jogszabályi környezetben is bizonytalanságot okoz.

Ezt észlelve korábban a NAIH ajánlásban foglalkozott a drónok használatára vonatkozó adatvédelmi kérdésekkel: többek között javasolta, hogy a jogalkotó írjon elő olyan azonosítási módszert a drónok üzemeltetőinek, használóinak, amelynek segítségével könnyen azonosíthatják az adatkezelő személyét a felvételeken szereplő emberek. Az "adatalanynak" egyértelmű tudomást kell szereznie arról, hogy a drón használója személyes adatainak kezelését mikor és hol kezdi, kezdheti meg. A Hatóság a drónhasználat törvényi szintű szabályozására tett javaslatot. A jogalkotó folytatott már bizonyos előkészületeket az önálló dróntörvény megalkotására, ezen folyamat azonban megakadt arra tekintettel, hogy a drónhasználat kérdései uniós szinten fognak szabályozásra kerülni.

8 Sütik adatkezelése

A süti a webszerver által küldött információcsomag, mely a látogató számítógépén előre meghatározott érvényességi ideig tárolódik. A sütik alkalmazása lehetőséget biztosít a látogató internethasználatának nyomon követésére, ezáltal meghatározható az érdeklődési köre, internet használati szokásai, honlap-látogatási története. A sütik így a látogató személyes adatainak hordozójaként kezelendőek, és ennek megfelelően az adatvédelmi jog szabályai is alkalmazandóak velük kapcsolatosan.

A SÜTIKKEL KAPCSOLATBAN A LÁTOGATÓKAT ÖSSZEFOGLALÓAN A KÖVETKEZŐRŐL KELL TÁJÉKOZTATNI:

– a süti neve,
– mely süti milyen adatokhoz fér hozzá,
– mi a süti élettartama,
– a süti funkciója, az adott süti miért szükséges a társaság számára vagy milyen funkciót nyújt a felhasználó részére.

Az adatkezelőnek egyes sütik esetében az érintett hozzájárulását kell kérnie azok alkalmazásához (minden süti esetében külön-külön). Ettől eltérően nem kell az érintett hozzájárulását kérni a honlap működéséhez feltétlenül szükséges sütik alkalmazásához, ekkor elegendő tájékoztatást nyújtani a sütik alkalmazásáról.

9 e-Pivacy Rendelet

Az e-Privacy Rendelet a GDPR-t kiegészítő, kifejezetten az elektronikus hírközlési ágazatban felmerülő személyes adatok kezelésére vonatkozóan fog a tagállamok számára közvetlenül alkalmazandó, kötelező iránymutatással szolgálni. A rendelet tervezete már elérhető, és elfogadása esetén a következő, jelen kiadvány szempontjából releváns területeket fogja várhatóan uniós szinten egységesen újraszabályozni:

– A főszabály szerint az elektronikus hírközlési adatok titkosak. Ezekhez hozzáférni, ezeket kezelni csak akkor lehet majd, ha azt az e-Privacy Rendelet megengedi.

– A hozzájárulás bármikor visszavonható marad, ugyanakkor a felhasználókat erre a szolgáltatóknak hathavonta emlékeztetnie is kell majd.

– A közvetlen üzletszerzési célú tájékoztatás nyújtásához, tehát online direkt marketing esetén előzetes hozzájárulásra van szükség. Akkor azonban, ha egy szolgáltató elektronikus levelezés céljából megszerzi ügyfeleitől elektronikus elérhetőségi adataikat egy termék vagy szolgáltatás értékesítése során, akkor ezeket – külön hozzájárulás nélkül – használhatja majd fel saját hasonló termékeivel vagy szolgáltatásaival kapcsolatos közvetlen üzletszerzési célra.

GDPR-kisokos kezdőknek

ALAPFOGALMAK

„SZEMÉLYES ADAT” – egy természetes személyre (az érintettre) vonatkozó bármely információ, például név, személyi szám, online azonosító vagy az érintett testi, gazdasági, kulturális vagy szociális jellemzői.

„ÉRINTETT” – bármely olyan természetes személy, aki valamely személyes adata(i) alapján közvetlenül vagy közvetve beazonosítható.

„ADATKEZELÉS” – a személyes adatokkal végzett bármely művelet, például a gyűjtés, rögzítés, rendszerezés, tárolás, megváltoztatás, lekérdezés, betekintés, felhasználás, közlés, továbbítás, terjesztés, törlés, illetve megsemmisítés.

„ADATKEZELŐ” – a személyes adatok kezelésére vonatkozó döntéseket (célok és eszközök) meghatározó személy vagy szerv.

„ADATFELDOLGOZÓ” – az adatkezelő nevében személyes adatokat kezelő személy vagy szervezet.

MI A KÜLÖNBSÉG AZ ADATKEZELŐ ÉS AZ ADATFELDOLGOZÓ KÖZÖTT?

Az adatkezelő a személyes adatok kezelésének céljait és eszközeit is meghatározza, az adatfeldolgozó pedig csak az adatkezelő által meghatározott célokat és eszközöket alkalmazva, az adatkezelő utasításainak megfelelően végrehajtja az adatkezelést. A megkülönböztetés célja elsődlegesen a felelősségi körök elhatárolása. Az adatfeldolgozó felel azért, hogy az adatkezelő által kijelölt körben végrehajtsa az adatkezelést, az adatkezelő pedig felel az adatkezelés jogszerűségéért.

ALAPELVEK

„JOGSZERŰSÉG, TISZTESSÉGES ELJÁRÁS ÉS ÁTLÁTHATÓSÁG”

„ADAT-TAKARÉKOSSÁG”

„CÉLHOZ KÖTÖTTSÉG”
– A személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történhet. A „majd jó lesz még valamire” stílusú adatgyűjtések és adatkezelések tehát nem megengedettek.

„PONTOSSÁG”

„KORLÁTOZOTT TÁROLHATÓSÁG”

„ELSZÁMOLTATHATÓSÁG”
– Az adatkezelő felelős a GDPR-ban és a hazai jogszabályokban foglaltaknak való megfelelésért, és képesnek kell lennie a megfelelés igazolására.

„INTEGRITÁS ÉS BIZALMAS JELLEG”

JOGALAPOK

„HOZZÁJÁRULÁS”
– például hírlevél küldés esetében.

„SZERZŐDÉS TELJESÍTÉSE”
– például a biztosított adatainak kezelése biztosítási szerződés esetén.

„JOGI KÖTELEZETTSÉG TELJESÍTÉSE”
– például munkaügyi adatkezelés esetében.

„LÉTFONTOSSÁGÚ ÉRDEKEK VÉDELME”
– például járványügyi célból történő adatkezelés esetében.

„KÖZHATALMI JOGOSÍTVÁNY GYAKORLÁSA”
– például az adóhatóság adatkezelése esetében.

„JOGOS ÉRDEK”
– például kamerás megfigyelőrendszer kiépítése és üzemeltetése esetében.

A HOZZÁJÁRULÁS BUKTATÓI

A GDPR nem elégszik meg azzal, hogy az érintett hozzájárulását adja az adatkezeléshez, hanem kifejezett követelményeket határoz meg a hozzájárulás érvényességével kapcsolatosan. Az érintett hozzájárulásának önkéntesnek, konkrétnak, megfelelő tájékoztatáson alapulónak és egyértelműnek kell lennie. A hozzájárulás kizárólag akkor lehet érvényes, ha valódi választási lehetőség áll az érintett rendelkezésére, tehát nem áll fenn becsapás, megfélemlítés vagy kényszerítés. Az adatkezelés célhoz kötöttségét és szükségességét hozzájárulás esetén is vizsgálni kell, így a cél nélkül vagy szükségtelenül végzett adatkezelés akkor is jogszerűtlen lesz, ha az érintett egyébként hozzájárulását adta.

JOGOS ÉRDEK – ÉRDEKMÉRLEGELÉSI TESZT

Amennyiben az adatkezelő vagy harmadik fél jogos érdekeinek érvényesítése képezi az adatkezelés jogalapját, az adatkezelő köteles meggyőződni arról (természetesen az adatkezelés megkezdése előtt), hogy a megjelölt jogos érdekkel szemben nem élvez-e elsőbbséget az érintett valamely jogos érdeke. Ennek legalkalmasabb eszközeként a GDPR az érdekmérlegelési tesztet jelöli meg. Ha az adatkezelő az adatkezelést megelőzően nem végezte el az érdekmérlegelési tesztet, a NAIH nem vizsgálhatja, hogy a teszt elvégzése jogszerűvé tehetné-e az adott adatkezelést. Mivel ezáltal kiemelt figyelem fordul a jogos érdek alapján végzett adatkezelésekre, fontos lehet, hogy az adatkezelő adatvédelmi szakértő bevonásával végezze el az érdekmérlegelés tesztjét.

HOLLÓ
VAS&FÜLÖP
ÜGYVÉDI TÁRSULÁS
+36 1 319 1201; +36 1 319 1279
office@hplaw.hu
www.hplaw.hu
/Holló Ügyvédi Iroda