Teendők az általános adatvédelmi rendelettel összefüggésben

Közel három hónapja, 2018. május 25. napjával vált alkalmazhatóvá a 2016/679.számú általános adatvédelmi rendelet (GDPR). Ennyi idő távlatából egyrészt értékes tapasztalatok vonhatóak le, melyeket érdemes elemzés alá venni, és röviden bemutatni. Másrészt pedig azt is célszerű bemutatni, hogy milyen lépések megtétele szükséges azon vállalkozások számára, melyek a megfelelést ennyi idő alatt sem valósították meg. Az alábbiakban ezen tapasztalatok és tanácsok kerülnek röviden és érthetően bemutatásra.

Fontos az adatvédelem, saját és ügyfélérdekeket is véd

Az adatvédelmi auditok alkalmával szinte minden esetben szóba kerül az ügyfelek részéről, hogy a GDPR kizárólag az ügyvédeknek jó, az a vállalkozások számára azonban inkább egy csapás. A gyakorlati tapasztalat azonban ezt egyértelműen cáfolja. A rendelet ugyanis semmi mást nem tűz ki célul, mint, hogy az érintettek, akiknek az adatait kezeljük, az adatkezelés részleteivel tisztában legyenek. Ennek pozitív következménye ugyanakkor az is, hogy **az adatkezelők számára is egyértelművé válik, hogy milyen személyes adatokat kezelnek, azokra ténylegesen szükségük van-e, azokat hol tárolják, megfelelően védik-e, valamint tudják-e, hogy kiknek és mikor továbbították.** Ezekre a kérdésekre ugyanis sok esetben az adatkezelők nem tudnak megfelelő válaszokat adni. Aki ugyanakkor a GDPR megfelelést megfelelően végrehajtotta, annak adatkezelései átláthatókká, áttekinthetőkké válnak, így nem kell továbbá attól rettegnie, hogy mi történik hatósági ellenőrzés vagy érintetti panasz/kérdés esetén.

A szabályozás bonyolult, laikusok számára nem áttekinthető

A GDPR szabályozási módja jellegében tér el az un. kontinentális szabályozási modelltől. Ez alatt azt kell értenünk, hogy az esetjogi alapú szabályozás kerüli a konkrét megfogalmazásokat és szabályokat, így az adatkezelőnek magának kell az adatkezelésekkel összefüggő folyamatos mérlegeléseket meghoznia, és a felelőséget felvállalnia. Nem ad pontos iránymutatást a rendelet például arra, hogy mely esetekben milyen jogalapot szükséges vagy lehetséges kiválasztanunk, mikor kell hatásvizsgálatot végeznünk, mely esetekben szükséges vagy ajánlott adatvédelmi tisztviselőt kijelölnünk, illetve hogyan osztályozzuk az adatvédelmi incidensek által jelentett egyes rizikókat. Valamennyi lényeges döntésben így magunknak kell döntést hoznunk. Ezek a döntések azonban bonyolult jogi összefüggésekre épülnek, melyek vonatkozásában mind az Európai Unió jogára, esetjogára, mind pedig a hazai jogra, NAIH gyakorlatra figyelemmel kell lennünk. Ezen joganyagok ugyanakkor egymással nem állnak minden esetben összhangban. Ilyen esetekben ugyanakkor érdemes a GDPR szabályait a Luxemburgi Bíróság és a NAIH értelmezései tükrében alkalmazni és az egyéb előírásokat háttérbe tenni. Nem segíti a tisztánlátást a sokak által várt Infotv. módosítása sem, hiszen annak szabályai többségükben nem a GDPR alatti adatkezelésekre vonatkoznak. Annak eldöntéséhez azonban, hogy mely szabályokról van szó (azaz mely előírásokat kell alkalmaznunk), az Infotv. rendelkezéseit soronként kell elemezni. Az előbbiek következtében a megfelelés megvalósítása kifejezetten komoly szakmai munka. Azoknak pedig, akik a vállalkozásuk adatkezeléseit át szeretnék látni vagy adatvédelmi tisztviselő pozíciót szeretnének betölteni, feltétlenül ajánlott megfelelő, lehetőség szerint több napos tanfolyam elvégzése.

A megfeleléshez régóta minden adott, kevés az új szabály

Meglepő módon azt tapasztalom, hogy a vállalkozások egy része a megfelelés megvalósítását a mai napig el sem kezdte. Ezzel összefüggésben több **téves alap**ra helyezik a bizalmukat. Ezeket érdemes bemutatni, hiszen az ellenőrzések - melyekre nem csupán érintetti panasz esetén kerülhet sor - nem kerülhetőek el.

A. "Nem végleges a szabályrendszer'

Egyrészt arra szokás hivatkozni, hogy a szabályrendszer nem végleges. Ezzel szemben a helyzet az, hogy az alapvető szabályokat a rendelet határozza meg, mellyel szemben tagállami jogszabály nem állhat, sőt azt nem is értelmezheti. Ebből eredően a rendelet szabályainak figyelembe vételével a megfelelés régóta teljes körűen megvalósítható. Az sem felel meg a valóságnak, hogy a rendelet teljesen új szabályokat vezetett be. A kötelezettségek jelentős része ugyanis már az Infotv. alapján is létezett, azokat az alacsony bírságokra tekintettel azonban nem követte senki.

B. "Mintaszabályzatokra várunk"

Valamennyi szakmában alapvető igény, hogy a kamarák a megfeleléshez szükséges mintákat bocsássák a tagok rendelkezésére. Ilyen igényt több munkáltatói szervezet is jelzett mind a NAIH, mind pedig a Pénzügyminisztérium felé. Ezen szervek azonban ezt az igényt nem tudják és nem fogják kielégíteni (nem is feladatuk). Ilyen minta ráadásul legfeljebb azok számára készíthető, akik egyedül dolgoznak alkalmazottak nélkül, tevékenységük sablonszerűen egyszerű, nem rendelkeznek honlappal és nincsenek kiterjedt üzleti kapcsolataik. Ellenkező esetben ugyanis az egyes adatkezeléseket egyenként (adatonként!) fel kell mérni, át kell vizsgálni, hogy az adatok honnan jönnek, hova mennek, hol kerülnek tárolásra, milyen adatbázisok képződnek, milyen üzleti kapcsolatok keretében kerülnek felhasználásra, kik kerülnek az adatkezeléssel összefüggésben bevonásra stb. Ezt követően a tényleges helyeztet át kell tekinteni a rendelet előírásai tükrében és azzal összhangba kell hozni. Végezetül pedig el kell készíteni a belső, külső tájékoztatókat, nyilvántartásokat, és módosítani szükséges a fennálló szerződéseket is.

C. "Én is értek hozzá"

Meg kellett tanulnunk az auditok során, hogy az adatvédelemhez mindenki ért. Picit olyan ez a helyzet, mint amikor a körzeti orvos felírja a gyógyszert, de mi megbeszéljük a családban, hogy a felírt gyógyszer szükségtelen, hiszen a panasz gyógyteával is kezelhető. S habár az ügyfélnek mindig igaza van, fel kell hívni a figyelmet arra kockázatokra és mellékhatásokra, azaz arra, hogy amennyiben például tévesen értelmezi a személyes adat fogalmát, a kezelhető adatok körét, a személyes adatok tárolására megszabható határidőt, az érdekmérlegelés vagy a hatásvizsgálat lényegét, 20.000.000,-EUR mértékű bírságra is számíthat.

Nincsen sem KKV kedvezmény, sem bírságtilalom, de ők is meg tudnak felelni

Megnyugtatóan hatott az adatkezelőkre, miszerint a NAIH első esetben figyelmeztetést fog alkalmazni. A Hatóság ugyanis az Infotv.75/A§ alapján az általános adatvédelmi rendelet 83. cikk (2)–(6) bekezdésében foglalt hatásköreit az arányosság elvének figyelembevételével gyakorolja, különösen azzal, hogy a személyes adatok kezelésére vonatkozó – jogszabályban vagy az Európai Unió kötelező jogi aktusában meghatározott – előírások első alkalommal történő megsértése esetén a jogsértés orvoslása iránt – az általános adatvédelmi rendelet

58. cikkével összhangban – elsősorban az adatkezelő vagy adatfeldolgozó figyelmeztetésével intézkedik. Ezzel összefüggésben utalnék **az Infotv.2§ (2) bekezdésére, mely szerint az Infotv. 75/A§-a a GDPR alatti adatkezelésekre NEM alkalmazható**.

A rendelet pontosan meghatározza a derogáció körét is. Eltérő szabályok alkalmazhatóak az egyházakra, az igazságszolgáltatási, bűnüldöző szervekre stb. Hasonló lehetőséget azonban a rendelet nem teremt a KKV-k számára. Három esetben tesz a rendelet a KKV-k számára könnyítést.

Az első eset a GDPR 30. cikke szerinti **belső nyilvántartás** esete. A kötelezettségek ugyanis nem vonatkoznak a 250 főnél kevesebb személyt foglalkoztató vállalkozásra vagy szervezetre, kivéve, ha az általa végzett adatkezelés az érintettek jogaira és szabadságaira nézve valószínűsíthetően kockázattal jár, ha az adatkezelés nem alkalmi jellegű, vagy ha az adatkezelés kiterjed a személyes adatok 9. cikk (1) bekezdésében említett különleges kategóriáinak vagy a 10. cikkben említett, büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó személyes adatoknak a kezelésére. Látható ugyanakkor, hogy ilyen egyszerű adatkezelés a való életben gazdasági tevékenység során nem fordul elő.

A következő eset a rendelet 24.cikk (2) bekezdésében nevesített **belső szabályrendszer** készítése alóli mentesítés. A rendelet szerint ugyanis erre csak akkor van szükség, ha az az adatkezelési tevékenység vonatkozásában arányos. Ezzel szemben az adatkezelőt az érintettek felé többségében előzetes (13.cikk), kivételesen utólagos tájékoztatási kötelezettség terheli (14.cikk). Ez pedig azt jelenti, hogy szabályrendszer készítésére szükség lesz.

Végezetül a **hatásvizsgálat**tal összefüggésben akként rendelkezik a GDPR, hogy a személyes adatok kezelése nem tekinthető nagymértékűnek (így emiatt nincsen szükség hatásvizsgálatra), ha az adatkezelés egy adott szakorvos, egészségügyi szakember betegei vagy egy adott ügyvéd ügyfelei személyes adataira vonatkozik. Ilyen esetekben az adatvédelmi hatásvizsgálatot nem kell kötelezővé tenni. A hatásvizsgálat ugyanakkor nem egy általános jogi kötelezettség, másrészt pedig meglehetősen szűk kört mentesít a rendelkezés. Az sem világos, hogy mi történik akkor, ha annak az egy szakembernek alkalmazottai is vannak (pl:ápoló).

A fentiek ellenére a mikrovállalkozások legnagyobb problémája nem a megfelelésre való képtelenség annak ellenére, hogy a hatályos szabályrendszer nyilvánvalóan nagy adatkezelőkre lett kialakítva. **A mikrovállalkozások adatkezelései ugyanis lényegesen egyszerűbben áttekinthetőek és kisebb jogi segítséggel, esetlegesen mintára támaszkodva a megfelelés megoldható.** A probléma itt a szakemberek hiányában mutatkozik meg, hiszen a kevés hozzáértő szakembert jelenleg is a nagyobb adatkezelők megfelelése köti le.

Aki még nem felelt meg, ezeket a lépéseket kövesse

Ahhoz, hogy a feladatainkat meg tudjuk határozni, tudnunk szükséges, hogy adatkezelőnek vagy adatfeldolgozónak minősülünk. A GDPR-ban meghatározott kötelezettségek zöme ugyanis az adatkezelő felelősségi körébe tartozik. **A könyvvizsgálók (hasonlóan az ügyvédekhez) ugyanakkor adatkezelőnek minősülnek, így számukra valamennyi**

kötelezettség teljesítendő. Munkájuk ugyanis nem pusztán, sőt alapvetően nem az ügyfél utasításai mentén történik, saját, alkalmazandó szabály- és felelősségrendszerük van, így adatfeldolgozóként való kezelésük nem felelne meg az adatvédelem alapvető elveinek.

A. Adatvagyonleltár készítése
Első lépésben fel kell mérni mindazon személyes adatok körét, amelyeket kezelünk. Ezzel összefüggésben tartsuk szem előtt, hogy minden adat, amely nálunk van (akár az irattárban vagy valamelyik gépünkön) adatkezelés alatt áll. Azt is meg kell vizsgálni, hogy ezeket a személyes adatokat mely rendszerekben tároljuk, azokhoz kik férnek hozzá, hova továbbítjuk őket.

B. Amely adatra nincsen szükségünk vagy nem jogszerű a kezelése, töröljük
Tekintettel arra, hogy az adatkezelők ez idáig gyűjtögető életmódot folytattak, bizonyára lesznek olyan adataink, melyekre vagy nincsen szükségünk (pl: régi életrajzok) vagy azokat nem kezelhetjük jogszerűen (pl: okirat másolatok). Ezeket sürgősen töröljük, illetve semmisítsük meg. Ez pedig mind az ügyféladatok, mind a munkavállalói adatok vonatkozásában jelentkező probléma. Utóbbit ugyanakkor a munka törvénykönyvének a módosítása esetlegesen orvosolhatja.

C. Hozzáféréskontroll, titkosítás
Vizsgáljuk meg, hogy az adatvagyonunkhoz pontosan kik és miért férnek hozzá. Biztosítsuk azt, hogy a munkavállalók közül sem férhet hozzá mindenki minden személyes adathoz, csupán azok, akiknek azzal konkrét teendőjük van. Személyes adatokat pedig ne küldözgessünk egymás között szükségtelenül, hiszen az adatkezelési időtartam lejártával valamennyi gépről és eszközről el kell majd távolítani ezen adatokat. Arra is figyeljünk, hogy a kifelé irányuló adatmozgások titkosítva történjenek. Ezzel ugyanis azt is biztosítani tudjuk, hogy téves adatküldés esetén ne kelljen az incidens magas kategóriába sorolnunk, így a NAIH-ot és az érintetteket értesítenünk. Természetesen erre (nem kell értesíteni) azért kerülhet sor, mert a titkosított személyes adatok hozzáférhetőségét megfelelően korlátoztuk, így a harmadik fél általi tudomásszerzést korlátoztuk. Ezzel pedig az érintettek adatait megfelelően megvédtük.

D. Belső és külső tájékoztatók készítése
Az érintetteket a személyes adataik kezeléséről tájékoztatni szükséges. A munkavállalókat un. belső, az ügyfeleket, szerződéses partnereket, érdeklődőket stb. külső adatkezelési tájékoztató útján tájékoztatjuk. Ezekben valamennyi adatkezelést be kell mutatnunk, azaz ismertetnünk kell a kezelt személyes adatokat, az adatkezelések jogalapját, célját, időtartamát, az adattovábbításokat és az érintetti jogokat. Ezen tájékoztatók elkészítése kifejezetten hosszadalmas munka, ne spóroljunk az energiánkkal. Az érintetteknek ugyanis valamennyi, általunk kezelt adatról tudomással kell rendelkezniük, így tehát az adatokat lényegében le kell könyvelnünk. Amennyiben pedig valamely adatra nincsen szükségünk vagy azt nem kezelhetjük, ahhoz az érintett hozzájárulását (engedélyét) sem kérhetjük.

E. Nyilvántartások készítése
Végezetül az adatkezeléseket le is könyveljük. Ennek megfelelően elkészítjük a GDPR 30. cikke szerinti belső nyilvántartást. Ezen felül mindenképpen szükségünk lesz egy

incidensnyilvántartásra is. Amennyiben pedig hírlevelet is küldünk az ügyfeleknek, un. opt-out nyilvántartást is vezetnünk kell.

Dr. Kéri Ádám
ügyvéd, adatvédelmi szakértő
A Pénzügyminisztérium kodifikációs bizottságának a tagja
Az MKVKOK, BDO, System Media, EDUCON oktatója