A GDPR egyszerűen kis- és középvállalkozások számára

A KKV-kézikönyv bemutatása

Előadásomban a GDPR kis- és középvállalkozások számára című kézikönyvet mutatom be, melyet a STAR II projekt keretében állították össze a Partnerek. 2020 decemberében a kézikönyv ingyenesen letölthető online formátumban elérhető lesz a Hatóság honlapján, továbbá 4.000 angol nyelvű példányt juttatunk majd el uniós KKV-k számára, valamint 2021 januárjában a Magyar Kereskedelmi és Iparkamara és Budapesti Kereskedelmi és Iparkamara segítségével 1.000 magyar nyelvű példányt az érdeklődő hazai KKV-khoz.

A KKV-k az Európai Unióban működő vállalkozások közel 99 százalékát teszik ki, ezzel ezek a vállalkozások a foglalkoztatás és a gazdasági növekedés motorjai. Ahogyan az előző előadásban is hallhattuk, a GDPR-nak való megfelelés mégis problémát okozhat a KKV-knak, mert az esetleges meg nem felelésük jelentős következményekkel járhat bírságok vagy az ügyfeleik bizalomvesztése képében.

A GDPR-megfelelés biztosítása és az ebből származó versenyelőny megszerzése az adatvédelmi alapelvek és az uniós adatvédelmi keretszabályozás megfelelő ismeretét igényli. Ez jelentős terhet ró a kisebb vállalkozásokra, különösen a kis- és középvállalkozásokra, mert habár a legtöbb KKV fő tevékenységi körébe nem tartozik bele, nem tudja elkerülni a személyes adatok kezelését.

A STAR II Konzorcium azzal a céllal állította össze a KKV-kézikönyvet, hogy könnyebben érthetővé tegye az Általános Adatvédelmi Rendeletet a kis- és középvállalkozások számára és támogassa ezeket a vállalkozásokat az adatvédelmi jogi kötelezettségeiknek való megfelelésben. Kiemelten fontos eszköze a KKV-k támogatásának, mert igyekszik közérthető nyelven tájékoztatást nyújtani a GDPR legfontosabb rendelkezéseiről, továbbá gyakorlati példákkal és jogesetekkel segíti a KKV-kat a GDPR-ból eredő kötelezettségeik megértésében.

A kézikönyv hozzáadott értéke

Több adatvédelmi hatóság bocsátott ki iránymutatásokat, némelyik kifejezetten KKV-knak szól. Azonban a projekt során lefolytatott interjúk során a KKV-k bírálták ezeket a dokumentumokat, és arról számoltak be, hogy nem igazán használják őket. Az elérhető iránymutatásokkal szemben azt a kritikát fogalmazták meg, hogy ezek az anyagok túlságosan általánosak és csak a jogelméletre fókuszálnak. A válaszadók rámutattak, hogy a felhasználóknak kell levonniuk a következtetéseket, és feltételezések alapján kénytelenek alkalmazni a Rendeletet egy adott helyzetben.

A kézikönyv hiánypótló útmutató az adatvédelmi megfeleléshez. Minden fejezete tartalmaz gyakorlati példákat, javaslatokat és további hasznos forrásokat is.

A kézikönyv összeállításának módszertana

Az útmutatóban szereplő témaköröket a STAR II projekt keretében azonosított, a KKV-kat leginkább foglalkoztató kérdéskörök alapján határoztuk meg. A projekt során interjúkat folytatottunk le adatvédelmi hatóságok képviselőivel, KKV-szövetségekkel és KKV-kal. További következtetéseket vontunk le KKV-k által kitöltött online kérdőívekből. A kézikönyvben meghatározott témakörök a KKV-hotline tapasztalatait követik.

A kézikönyv szerkezete

Az **I. fejezet (Az adatvédelmi szabályozás térképe)** áttekintést nyújt az európai adatvédelmi terület főbb szereplőiről, bemutatja szerepüket és felelősségi körüket, és kitér arra, hogy milyen módon tudják segíteni a KKV-kat a GDPR-ból eredő kötelezettségeiknek való megfelelésben.

A GDPR alapelv-központú szabályozást tartalmaz, és minden vállalkozásnak lehetőséget biztosít arra, hogy a számára legmegfelelőbb megfelelési stratégiát dolgozza ki. A stratégia kialakítása, priorizálás és az intézkedések megtervezése során számos segítség áll a KKV-k rendelkezésére. Ezek közül néhányat a felügyeleti hatóságok, néhányat a magánszektor bocsátott ki. Az információgyűjtés során nagyon fontos, hogy megbízható forrásokra támaszkodjunk!

Például használjuk a nemzeti és regionális adatvédelmi hatóságok által kibocsátott iránymutatásokat.

Tekintve, hogy a GDPR az EU egész területén alkalmazandó, a KKV-k székhelyüktől függetlenül bármely uniós felügyeleti hatóság által kiadott sablont és eszközt felhasználhatják, feltéve, hogy az iránymutatást (amennyiben szükséges) hozzáigazították a nemzeti szabályozáshoz.

Felhasználhatjuk az Európai Adatvédelmi Testület (EDPB), az Európai Adatvédelmi Biztos (EDPS) vagy az Európai Uniós Kiberbiztonsági Ügynökség (ENISA) útmutatóit is. Utóbbi a hálózati- és információbiztonsági problémák kezelésében, megoldásában és megelőzésében támogatja az európai intézményeket, tagállamokat és vállalkozásokat. Érdemes az Európai Unió Alapjogi Ügynöksége (FRA), és az Adatvédelmi Szakemberek Nemzetközi Szövetsége (IAPP) által kibocsátott iránymutatásokat is figyelemmel kísérni.

A **II. fejezet (Adatvédelmi alapismeretek)** ismerteti az adatvédelmi szabályozás hatályát és a KKV-kra vonatkozó rendelkezéseit. A fejezet a leggyakrabban felmerülő kérdések megválaszolásával bemutatja az adatvédelmi szabályozás középpontját jelentő fogalmakat és alapelveket. Az adatvédelmi megfelelési stratégia kidolgozásához elengedhetetlen ezek magas szintű ismerete. A gyakran ismételt kérdéseket a NAIH által üzemeltetett KKV- hotline-ra beérkező kérdések alapján állította össze a Konzorcium.

Mindenekelőtt a személyes adat és az adatkezelés fogalmát tisztázza, és támasztja alá az útmutató, hiszen ezen fogalmak ismerete elengedhetetlen a GDPR-nak való megfelelő adatkezelés kialakításához.

Adatkezelésnek minősül, ha

- egy fodrász ügyfelei nevét, keresztnevét, telefonszámait tartalmazó jegyzetet vezet;
- egy panzió tulajdonosa Excel táblázatban jegyzi fel a vendégek foglalásait és elérhetőségeit;
- a beteg alkalmazott munkaadója továbbítja az alkalmazott adatait a felelős hatósági szervnek;
- az állásra jelentkezők önéletrajzát átnézi a fejvadász;
- a KKV telefonszámokat és e-mail címeket gyűjt honlapokról direkt marketing üzenetek küldése céljából.

A kézikönyv következő szakasza ismerteti, hogy milyen szerepet tölthet be egy KKV az adatkezelési tevékenységekben.

A KKV-k GDPR-ból eredő kötelezettségei az adatkezelésben betöltött szerepüktől függően változnak.

Három lehetőség merülhet fel:

- a KKV lehet (önálló vagy közös) adatkezelő és saját maga végezheti az adatkezelési tevékenységet,
- megbízhat egy másik vállalkozást, az adatfeldolgozót, hogy a nevében dolgozzon fel személyes adatokat, vagy

- egy másik vállalkozás megbízásából kezel személyes adatokat, így adatfeldolgozóként jár el.

Az adatkezelők elsődleges felelősséggel bírnak az adatkezelés, valamint az adatvédelmi követelményeknek és alapelveknek való megfelelés tekintetében, és ők tehetők felelőssé az adatkezelésből eredő bármilyen kár okozásáért, azonban a GDPR értelmében az adatfeldolgozóknak is teljesíteniük kell bizonyos jogi kötelezettségeket.

PÉLDA
Egy gyógyfürdő és egy kozmetikus külön jogi személyek, de egy helyen nyújtanak szolgáltatást. Közös hűségprogramot indítanak (például a fürdőbelépő 5% kedvezményre jogosít a kozmetikusnál, és a kozmetikusnál 10.000 HUF feletti vásárlás esetén 5% kedvezmény jár a fürdőbelépő árából). A hűségprogramba való belépéshez az ügyfeleknek meg kell adniuk a nevüket, keresztnevüket és e-mail címüket. A közös hűségprogram során végzett adatkezelés tekintetében a kozmetikus és a fürdő közös adatkezelőnek minősül, ha együttesen határozták meg az adatkezelés lényeges kérdéseit, vagy ha külön-külön mindkét félnek érdemi ráhatása volt az adatkezelés kialakítására.
A kézikönyv bemutatja az adatkezelés alapelveit is.

Az alapelveket felfoghatjuk a jogrendszer különösen fontos értékeit magukban foglaló általános normákként. A GDPR hat alapelvet fogalmaz meg az adatkezelésre vonatkozóan, melyeknek az adatkezelők kötelesek megfelelni:

1) Jogszerűség, tisztességes eljárás és átláthatóság
2) Célhoz kötöttség
3) Adattakarékosság
4) Pontosság
5) Korlátozott tárolhatóság
6) Integritás és bizalmasság

Mi lehet az adatkezelés jogalapja?

A jogszerű adatkezelés érdekében a KKV-knak megfelelő jogalappal kell rendelkezniük a személyes adatok kezeléséhez.

A GDPR 6. cikke az alábbi lehetséges jogalapokat határozza meg:

- az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez;
- az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél;
- az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges;
- az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges;
- az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges;
- az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé, különösen, ha az érintett gyermek.

Hogyan válasszuk ki a megfelelő jogalapot?

A megfelelő jogalap kiválasztása az adatkezelési tevékenységek körülményeitől függ.

- Hozzájárulás

A hozzájárulás beszerezhető az érintettől nyilatkozat útján (írásos, szóbeli, képi vagy hang stb.) vagy megerősítő cselekedettel (kattintás, számjegy beírása stb.). A GDPR nem határozza meg a hozzájárulás formáját, így az elektronikusan is megadható, de az adatkezelőnek képesnek kell lennie a hozzájárulás megadásának bizonyítására.

A hozzájárulás érvényességének feltétele, hogy az az adatalany önkéntes, konkrét, tájékoztatáson alapuló és egyértelmű kinyilatkoztatása legyen, amellyel hozzájárul személyes adatai kezeléséhez.

A gyakorlatban önkéntes hozzájárulásnak minősül, ha az adatalany arról szabadon dönthet, azaz a hozzájárulás megadását megtagadhatja vagy bármikor visszavonhatja anélkül, hogy bármilyen hátrány érné emiatt. Ilyen hátrány például a megtévesztés, megfélemlítés, kényszerítés, vagy egyéb jelentős következmény. Az adatalanyra nézve elhanyagolható negatív következmények nem veszélyeztetik a hozzájárulás érvényességét. Egy kisbolt vásárlói kártyákat ad a vásárlóinak, hogy kedvezményeket gyűjthessenek. Ebben az esetben a kisbolt kezelheti a vásárlók adatait hozzájárulás alapján, mert a kedvezményektől való elesés nem jár jelentős negatív következménnyel a vásárlókra nézve.

Feltehetően nem tekinthető önkéntesnek a hozzájárulás, ha az az általános felhasználási feltételekbe van beágyazva, és nem választás kérdése, valamint – főszabály szerint – kiegyensúlyozatlan erőviszonyokban sem (például munkaviszonyban). Egy munkáltató kamerákat szerel fel a munkahelyen, amelyhez a munkavállalók hozzájárulását kéri. A munkavállalók egyértelműen nincsenek abban a helyzetben, hogy a kamerák felszereléséhez szabadon hozzájárulást adjanak, illetve hátrányos következményekkel járna, ha a hozzájárulást megtagadnák. Az adatkezelőnek ebben az esetben más jogalapot kell választania.

A *„kifejezett hozzájárulás”* azt jelenti, hogy ha az adatkezelés több célt szolgál, a hozzájárulást minden egyes adatkezelési cél vonatkozásában be kell szerezni. Ezt nevezzük tagolt hozzájárulásnak.

PÉLDA
Egy sportközpont szeretné összegyűjteni a vásárlói e-mail címét, hogy havi hírlevelet küldhessen nekik az új edzésekről és képzésekről. A sportközpont a vásárlók e-mail címét további partnervállalataival is meg szeretné osztani (például fitnesz ruházatot gyártó vállalat, kiegészítőket forgalmazó vállalat). Ebben az esetben a sportközpontnak mindkét adatkezelési célhoz, azaz a hírlevél küldéséhez és az e-mail címek másik vállalatnak történő továbbításához is külön-külön be kell szereznie a hozzájárulást.

TIPP
Nem minden esetben megfelelő vagy célszerű a hozzájárulást választani az adatkezelés jogalapjának. Kihívást jelent annak bizonyítása, hogy a hozzájárulás önkéntes, konkrét, tájékoztatáson alapuló és egyértelmű, ezért amennyiben lehetséges, ne féljünk másik jogalap alkalmazásától!

- Szerződéses jogviszony

Bizonyos esetekben az adatkezelés olyan szerződés teljesítéséhez szükséges, melyben az érintett az egyik fél.

PÉLDA
Egy online boltnak termékei kiszállításához kezelnie kell a vásárlók lakcímadatait. Ebben az esetben az adatkezelés jogalapja az eladó és a vevő között kötött adásvételi szerződés teljesítése, melynek érdekében szükséges a lakcím ismerete.

- Jogi kötelezettség teljesítése

Bizonyos esetekben az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges. A jogi kötelezettség eredhet uniós vagy tagállami jogból is. A jogszabálynak ebben az esetben meg kell határoznia az adatkezelés célját, az adatkezelő kilétének megállapítását, a kezelendő adatok és érintettek, valamint azok körét, akikkel a személyes adatokat közlik.

PÉLDA
Az adatkezelés jogalapja a jogi kötelezettség teljesítése, ha egy vállalkozás a vásárlói adatait megküldi az adóhivatalnak, vagy ha az alkalmazottai társadalombiztosításhoz szükséges személyes adatait megküldi az illetékes nemzeti hatóságnak.

- Az érintett vagy egy másik természetes személy létfontosságú érdeke

Bizonyos esetekben az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges. Az adatvédelemhez való jog alapvető, de nem kizárólagos, élet-halál kérdésében a személyes adatok védelméhez való jogot természetesen felülbírálja az élethez való jog.

PÉLDA
Egy munkahelyi baleset esetén a munkaadó közölheti a munkavállaló személyes adatait a sürgősségi ellátást végző orvosokkal.

- Közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges

Bizonyos esetekben az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges.

Kivételes esetben egy KKV-t a rá vonatkozó jogi szabályozás értelmében megbízhatnak közérdekű vagy közhatalmi jogosítvány gyakorlásának keretében végzett feladattal. Amennyiben ezen feladatok ellátásához a KKV-nak személyes adatokat kell kezelnie, közérdek vagy a közhatalmi jogosítvány gyakorlása lehet az adatkezelés jogalapja.

PÉLDA
Egy busztársaság biztosítja a közösségi közlekedést egy városban. A cég munkatársai a jegyellenőrzés során a bírság kiszabásához elkérhetik a jegy nélkül utazók elérhetőségét. A jogalap ebben az esetben közhatalmi jogosítvány gyakorlása.

- Az adatkezelő jogos érdeke

Bizonyos esetekben az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, azonban ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek a személyes adatok védelmét teszik szükségessé, különösen, ha az érintett gyermek.

A jogos érdek alkalmazásának feltétele, hogy az adatalany az adatgyűjtés időpontjában a gyűjtött adatok vonatkozásában joggal számíthat arra, hogy az adatok kezelésére a meghatározott cél érdekében sor kerülhet. Ha a személyes adatok kezelése egy csalás megelőzése érdekében feltétlenül szükséges, ez az adatkezelő jogos érdekének számít.

PÉLDA
Egy vállalkozás ételházhozszállítási szolgáltatást nyújt. Az új vásárlók ajándék ételt kapnak házhozszállítással. Az ajánlatot egy háztartás csak egyszer veheti igénybe, ezért a vállalkozás a már meglévő ügyfeleiről vezetett nyilvántartását összeveti az új ügyfelek adataival, hogy ne történhessen visszaélés.

A KKV-k és az adatvédelmi tisztviselő

A GDPR elfogadásával az adatkezelők és adatfeldolgozók is kötelesek adatvédelmi tisztviselőt kinevezni. A széles körben elterjedt nézettel szemben az adatvédelmi tisztviselő kinevezésére vonatkozó jogi kötelezettség szempontjából nem a vállalkozás mérete, hanem az annak fő tevékenységéhez nélkülözhetetlen adatkezelési tevékenység nagysága a döntő. Ezek azok az adatkezelési tevékenységek, melyek alapvető fontosságúak a vállalkozás céljainak eléréséhez. Az adatvédelmi tisztviselő kinevezése ezért – bár nem gyakran fordul elő, de alapvetően – az adatkezelő és adatfeldolgozó KKV-kra is vonatkozik. Választhatnak, hogy belső (saját munkatárs) vagy külső (adatvédelmi tisztviselői szolgáltatás) adatvédelmi tisztviselőt neveznek ki.

PÉLDA
A KKV köteles adatvédelmi tisztviselőt kinevezni, ha telekommunikációs hálózatot üzemeltet, fitnesz és egészségügyi adatokat figyel meg applikációkon keresztül vagy hűségprogramok, viselkedésalapú hirdetések esetén. Köteles DPO-t kinevezni a vérvizsgálatokat végző labor, egy klinika (ha nem egy adott szakorvos, egészségügyi szakember betegeiről van szó) és egy társkereső applikációt üzemeltető KKV is.

Az adatvédelmi tisztviselő lehet a KKV alkalmazottja vagy külső szakértő is, de mindkét esetben alapvető fontosságúak a függetlenségét biztosító feltételek:

- Legyenek biztosítottak számára azok a források, amelyek feladatai végrehajtásához szükségesek, azaz pénz, munkaerő, (szakmai fejlődésre fordítható) idő;
- Az adatvédelmi tisztviselő feladatai ellátásával kapcsolatban utasításokat senkitől ne fogadjon el;
- Az adatkezelő vagy az adatfeldolgozó az adatvédelmi tisztviselőt feladatai ellátásával összefüggésben nem bocsáthatja el, és szankcióval nem sújthatja;
- Az adatvédelmi tisztviselő közvetlenül az adatkezelő vagy az adatfeldolgozó legfelső vezetésének tartozik felelősséggel; valamint
- Az adatvédelmi tisztviselő feladataiból nem fakadhat összeférhetetlenség (például az adatkezelés tárgyának és céljainak meghatározása, a KKV képviselete jogi eljárásokban).

Amennyiben az adatvédelmi tisztviselő a vállalkozás alkalmazottja, függetlenségének biztosítása érdekében mindig tisztázni kell, hogy éppen adatvédelmi tisztviselői szerepében jár-e el.

A **III. fejezet (A kockázatalapú megközelítés az elméletben és a gyakorlatban)** bemutatja a GDPR kockázatalapú megközelítést tartalmazó rendelkezéseit. A fejezet ismerteti az adatkezelő feladatait (GDPR 24. cikk), a beépített és alapértelmezett adatvédelem alapelvét (GDPR 25. cikk), a biztonsági követelményeket (GDPR 32. cikk), az adatvédelmi incidensre és az érintett tájékoztatására (GDPR 33. és 34. cikk), az előzetes adatvédelmi hatásvizsgálatra (GDPR 35. cikk), és az előzetes konzultációra (GDPR 36. cikk) vonatkozó szabályokat. A fejezet utolsó szakasza a magatartási kódexeket (GDPR 40. cikk) és a tanúsításokat ismerteti (GDPR 42. és 43. cikk).

A GDPR 30. cikke az adatkezelési tevékenységek nyilvántartásáról

Az adatkezelési tevékenységekről írásos formában kell dokumentációt vezetni. Az adatkezelő (és az adatfeldolgozó) választhat, hogy papíralapon vagy elektronikus formában teszi ezt meg.

A KKV-k mentesülnek a nyilvántartási kötelezettség alól az alábbi feltételek fennállása esetén:

- az adatkezelés az érintettek jogaira és szabadságaira valószínűsíthetően nem jár kockázattal;
- az adatkezelés alkalmi jellegű (azaz nem rendszeres vagy folyamatos); vagy

- az adatkezelés nem terjed ki a személyes adatok különleges kategóriájának vagy a büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó személyes adatoknak a kezelésére.

A gyakorlatban csak kevés KKV felel meg teljesen ezeknek a feltételeknek.

PÉLDA

- Ha a vállalkozásnak 250 főnél kevesebb alkalmazottja van, akkor is nyilvántartást kell vezetnie a munkavállalók adatainak kezeléséről, mert az adatkezelés nem alkalmi jellegű, és az alkalmazottak személyes adatai között különleges adatok is szerepelnek (például táppénz esetén).
- Egy tetoválószalon nyilvántartást vezet az ügyfelei egészségügyi adatival kapcsolatos adatkezelésekről.

Ha a KKV mentesül is a nyilvántartás-vezetési kötelezettség alól, javasolt nyilvántartást vezetni az alkalmi jellegű adatkezelésekről, mert egy esetleges ellenőrzés során sokkal könnyebben együtt tud működni a felügyeleti hatósággal, és igazolni tudja a GDPR-nak való megfelelését.

Az adatkezelési tevékenységekről vezetett nyilvántartás mellett az egyéb nyilvántartásokat is célszerű írásos formában vezetni, mert ezek segítségével az adatkezelők és adatfeldolgozók igazolni tudják, hogy megfelelnek a GDPR rendelkezéseinek.

Kifejezetten javasolt nyilvántartást vezetni az alábbiakról:

- adatvédelmi kockázatok;
- írásos szerződések megkötése a (közös) adatkezelők, az adatkezelők/adatfeldolgozók, valamint az adatfeldolgozók/alvállalkozók között, melyben meghatározzák a kölcsönös felelősségi köröket,
- az adatvédelmi tisztviselő javaslatai (írásos vélemények, e-mailek stb.),
- az adatvédelmi tisztviselő kinevezéséről (vagy ennek mellőzéséről) hozott döntés,
- az adatkezelési tevékenység különböző fázisaiban hozott technikai és szervezési intézkedések,
- az előzetes adatvédelmi hatásvizsgálat folyamatainak rögzítése,
- az adatvédelmi incidensek/ezek okai/ hatása/orvoslásukra tett lépések,
- az érintettek jogait garantáló intézkedések,
- az adatkezelési alapelveknek való megfelelés érdekében hozott intézkedések,
- az adatkezelés joglapjai és azok felülvizsgálata.

A kézikönyv **IV. fejezete (Sajátos adatkezelési tevékenységek)** a munkavállalók személyes adatainak kezelésre vonatkozó szabályokat mutatja be, melyről a konferencia 2. paneljében hallhatnak előadást.