GDPR KKV munkafüzet

Ez a munkafüzet a KKV szektor sajátos igényeihez igazított GDPR megfelelést segítő eszköz, amelynek célja, hogy az erőforrásaiban korlátozott vállalkozások is kielégítő módon megfeleljenek az adatvédelmi rendelet alapvető elvárásainak. A munkafüzet olyan vállalkozásokat céloz meg, amelyek adatkezelésükben jellemzően egyszerűek, ám a rendelet általános hatálya miatt mégis alanyai a szabályozásnak. A jelenlegi szabályok alapján a GDPR lényegében minden vállalkozást érint.

A munkafüzet önmagában feldolgozható, de a kapcsolódó előadás nagyban segíti a helyes használatát, így azt javasoljuk megtekintésre. Ezeket az előadások jellemzően kamarai szervezésben elérhetőek, érdeklődjön a helyi kamaránál vagy az tibor@zenit-services.com email címen. A munkafüzet szabadon másolható, de kereskedelmi céllal nem használható, azaz pénzért nem árusítható.

A munkafüzet kérdéseket tesz fel a vállalkozásnak, amelyeket az a munkafüzetben megválaszol. A kérdések vizsgálata és a felelős válaszadás véleményünk szerint alkalmas eszköz annak bizonyítására, hogy a vállalkozás érdemben foglalkozott az adatvédelmi rendelettel. Ez egy szerény adatkezelési portfólióval rendelkező KKV esetén véleményünk szerint elégséges a GDPR megfeleléshez, de természetesen nem alkalmas, összetett és nagy léptékű adatkezelést megvalósító vállalkozások felméréséhez.

A munkafüzet az általános adatvédelmi rendelet jelenlegi állását veszi figyelemben (2018. március).

A munkafüzetben egyrészt IGEN/NEM kérdéseket találhat az olvasó. Ezeknél kérjük jelölje meg, vonatkozik-e az adott állítás a vállalkozására. Máshol kitöltendő adatokat talál, ott ezekről tájékoztatást adunk.

A munkafüzet kitöltője

Vállalkozás neve	
Címe	
Kitöltő neve	
Pozíciója	

I. Különleges adatkezelési esetek

Az első fejezetben kizárjuk a különleges adatkezelési eseteket. Ez csak a vállalkozások kis részét érinti, de fontos tisztába lennünk velük. Az alant felsorolt speciális esetek különös figyelmet igényelnek adatkezelés szempontjából, így ha bármelyik kérdésre a válasz IGEN, a munkafüzet nem lesz elégséges segítség, javasoljuk hogy konzultáljon egy GDPR tanácsadóval.

I/a. Különleges kategóriájú adatok kezelése

Vannak olyan különösen érzékeny adatok, amelyeknek a kezelése mindenképpen speciális igényeket támaszt, például adatvédelmi tiszt alkalmazását és szigorú adatvédelmi intézkedéseket, a vállalkozás méretétől függetlenül. Ez a 9. cikkely szerint:

A faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a természetes személyek egyedi azonosítását célzó genetikai és biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok.

Kezel az ön vállalkozása különleges kategóriájú adatot?	IGEN	NEM

I/b. Büntetőjoggal összefüggő adatkezelés

A 10. cikkely említi a büntetőjoggal kapcsolatos adatkezelést is. *A büntetőjogi felelősség megállapítására vonatkozó határozatokra és a bűncselekményekre vonatkozó személyes adatok kezelése* is külön intézkedéseket kíván.

A ön vállalkozása kezel adatokat büntetőjogi felelősség megállapításával vagy bűncselekményekkel összefüggésben?	IGEN	NEM

I/c. Közhatalmi szervek vagy egyéb, közfeladatot ellátó szervek

Az említett szervek, kivéve az igazságszolgáltatási feladatkörükben eljáró bíróságokat, külön rendelkezéseknek kell megfelelnie.

A ön vállalkozása lát el közhatalmi funkciót vagy közfeladatot?	IGEN	NEM

I/d. Az érintettek rendszeres és szisztematikus, nagymértékű megfigyelését teszik szükségessé

A rendelet szerint, különleges eset, ha *az adatkezelő vagy az adatfeldolgozó fő tevékenységei olyan adatkezelési műveleteket foglalnak magukban, amelyek jellegüknél, hatókörüknél és/vagy céljaiknál fogva az érintettek rendszeres és szisztematikus, nagymértékű megfigyelését teszik szükségessé*.

A rendelet nem teljesen egyértelmű, egyéb iránymutatások alapján, a nagymértékű tipikusan egy magánpraxis ügyfélszámosságát meghaladó mennyiségben, a szisztematikus pedig a rendszeres, visszatérő, adott logikát követő megfigyelést jelenti. Ilyen például telekommunikációs rendszer üzemeltetése, profil alapú marketing emailek küldése, hitelképesség besorolás, biztosítási kedvezmény adása, stb.

Végez-e az ön vállalkozása rendszeres, szisztematikus nagymértékű megfigyelést?	IGEN	NEM

I/e. Magas kockázatú adatkezelés

Ha az adatkezelés valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira, különösképpen ha új technológiákról van szó, hatásvizsgálatra és hatósági konzultációra lehet szükség. Ez a hétköznapi adatkezelésekre jellemzően nem vonatkozik, ha a technológia és gyakorlati adatvédelmünk az

általános gyakorlatnak megfelel. Ez a kitétel elsősorban az új technológiák, profilozások bevezetőire vonatkozik.

Végez-e olyan adatkezelést, ami magas (és nem mérsékelhető) kockázattal jár?	IGEN	NEM

I/f. Személyes adatok harmadik országba továbbítása

Amennyiben az adatokat külföldre vagy nemzetközi szervezetnek továbbítjuk, meg kell vizsgálni, hogy az adott ország vagy szervezet megfelelő-e az adatvédelmi elvárásoknak.

Nagyon leegyszerűsítve, az Európai Unión belül, az országok adatkezelése és demokráciájuk fejlettsége megfelelő ehhez. Ha az EU-n kívülre továbbítjuk a személyes adatokat, akkor vizsgálandó, hogy ez az ország megfelel-e az elvárásoknak. Ezt a adatvédelmi Bizottság határozza meg. Természetesen a fejlett, demokratikus országok ennek jellemzően megfelelnek (pl USA), míg a kétséges kormányzás alatt álló országok kevésbé.

Továbbít az Európai Unión kívülre, nem „megfelelő” országba személyes személyes adatokat?	IGEN	NEM

I/g. Automatizált döntéshozatal

A rendelet külön foglalkozik az úgynevezett automatizált döntéshozó rendszerekkel. Az olyan rendszerek, amelyek emberi beavatkozás nélkül döntenek a személyt jelentős mértékben érintő dolgokról, mint például biztosítási besorolás, hitelbírálat, stb, külön szabályoknak kell megfelelni.

Van önnek olyan rendszere ami automatizált döntéseket hoz az adat alanyokról?	IGEN	NEM

I/h. Gyerekeknek nyújtott információs társadalommal összefüggő szolgáltatás

A potenciálisan gyerekeknek nyújtott online szolgáltatások esetén különleges eset lehet, ha az alábbiak mindegyik igaz:

- Információs társadalommal összefüggő szolgáltatás (online szolgáltatás, pl közösségi oldalak)
- 16 éven aluliak igénybe vehetik (Magyarországon 16, más országokban esetenként alacsonyabb korhatár)
- Hozzájáruláson alapuló adatkezelésről van szó (és nem szerződés alapú)

Ilyen szolgáltatás esetén, szülői hozzájárulásra lehet szükség. Nagyon sok szolgáltatást és kapcsolódó adatkezelést szerződés teljesítésekor hajtunk végre (pl. webshop vásárlás), azokat ez nem érinti. Az is előfordulhat, hogy ha mégis hozzájárulást kérünk valamihez, de kijelentjük, hogy csak 16 éven felüliek vehetik igénybe azt a szolgáltatást.

Nyújt-e 16 éven aluliaknak hozzájárulás alapján történő információs társadalommal összefüggő szolgáltatást?	IGEN	NEM

I/i. Első fejezet összegzése

A fenti kérdések a GDPR speciális eseteivel vannak összefüggésbe. Ha bármelyik kérdésre IGEN-nel válaszoltunk, akkor érdemes GDPR tanácsadót felkeresnünk. Lehet, hogy a rendelkezés tekintetében elég egy adatvédelmi tisztviselőt kijelölni, vagy hatásvizsgálatot elvégezni, ám jellemzően az ilyen speciális esetek kapcsán történő adatkezelésnél az éppen hogy elégséges erőfeszítést nem fogja a hatóság elfogadni. Ilyen esetekben javasoljuk, hogy az érintett vállalkozások kimerítően dokumentálják az adatvédelmi gyakorlatukat.

II. Az adatkezelés lehetséges jogalapja

A rendelet megköveteli, hogy a személyes adatok kezelése során mindig meg tudjunk nevezni jogalapot. Ezek listája, a sor elején a leggyakoribb és legjobb jogalapokkal:

- Szerződés teljesítése. Ilyen lehet a munkáltatói szerződés, de egy vásárlás a webshopban is. A legkevesebb problémával járó jogalap.
- Jogi kötelezettség teljesítése. Ilyen lehet a számviteli törvény (mennyi ideig tartjuk meg a számlákat) vagy más helyi rendelkezés.
- Hozzájárulás alapján. Azaz az adat alany, valamikor, valamilyen bizonyítható módon hozzájárult az adatkezeléshez. Tudnunk kell bizonyítani, hogy ez megtörtént.
- Jogos érdek alapján. A vállalkozás azonosít valamilyen jogos érdeket (azaz a vállalkozás érdekét), amit mérlegelés után erősebbnek ítél az adat alany érdekeinél. Ez problémás jogalap, ennek kapcsán javasoljuk, hogy konzultáljanak szakértővel.
- Létfontosságú érdek, például a személy biztonsága, életvédelme kapcsán kezelt adat.
- Közérdekű vagy közhatalmi jogosítvány gyakorlásához kapcsolódó adatkezelés.

A jogalapot feltüntethetjük az *adatleltárban*, de adatleltárt nem kötelező készíteni. Szintén feltüntethetjük a lejjebb említett *adatvédelmi tájékoztatóban*, de legfontosabb, hogy a hatóság vizsgálata esetén meg tudjuk őket nevezni.

Az Ön vállalkozásában milyen jogalap alapján kezelnek adatokat?

Szerződés teljesítése	
Jogi kötelezettség teljesítése	
Hozzájárulás alapján	
Egyéb:	

III. GDPR jogok elérhetővé tétele

A rendelet legfontosabb újdonsága, hogy az adat alanyoknak (azaz a természetes személyeknek) számos jól meghatározott új joga van és az adatkezelőnek felelőssége, hogy ezeket a jogokat érvényesíteni tudják. Ebben a fejezetben ezeket a jogokat vizsgáljuk meg és azt, hogy miként tudunk ennek megfelelni.

A GDPR jogok, röviden összefoglalva, arról szólnak, hogy az adat alany a tulajdonosa a róla szóló adatoknak. Ennél fogva, kérheti, hogy mutassuk meg, milyen információink vannak róla, elrendelheti azok helyesbítését. Bizonyos esetekben kérheti azok törlését (amennyiben ez lehetséges) vagy éppen az adatkezelés felfüggesztését, illetve tiltakozhat az adatkezelés ellen.

A jogok biztosítása bonyolultnak tűnhet első ránézésre, de valójában bőven elégséges lehet egy ezzel foglalkozó munkatárs elérhetőségét megadni, aki akár manuális módon intézkedhet a jogérvényesítésről (pl adat törléséről). A várakozás az, hogy a legtöbb KKV esetében a nullához közelítő mennyiségben fog ilyen megkeresés történni. Így azoknak a KKVéknak, akik nem kezelnek összetett és nagy léptékű személyes adatbázisokat, pontosan ezt javasoljuk. Jelöljenek ki egy adminisztrációs munkatársat, aki elérhető a GDPR jogok kapcsán. Erről cégen belül tájékoztathatjuk a dolgozókat egy körlevélben, vagy faliújságon, a vevőinket pedig a honlapunkon, például egy *adatvédelmi információk* fülön. Az intézkedésre a rendelet normális esetben egy hónapot ad, ami bőségesen elég ahhoz, hogy kézi módszerekkel megoldja a cég a kéréseket.

Természetesen komplex és nagy léptékű rendszerek esetén, ajánlott lehet az egyes funkciók automatizálása.

III/a. Rendelkezésre bocsátandó információk

Az adat alanynak lehetőséget kell biztosítani arra, hogy tájékozódjon a jogairól és arról, hogy mi történik az adataival. Ennek formai követelménye nincs, lehet akár szóbeli tájékoztatás is egy munkaszerződés aláírásakor, de általában érdemesebb ezt írásban megtenni, így könnyen bizonyítható, hogy a tájékoztatás megtörtént.

Széles körben elérhető szolgáltatások esetén (pl. webshop), szenteljünk egy oldalt az *adatvédelmi információknak*, ahol kimerítően értekezünk cégünk gyakorlatáról.

A tájékoztatás keretében az alábbi információkat kell átadnunk:

- Az adatkezelő kiléte és elérhetőségei (cégnév, cím, email, telefonszám)
- Ha van adatvédelmi tisztviselő, az ő elérhetőségét (jellemzően KKVéknál nincs)
- A személyes adatok tervezett kezelésének célja és jogalapja
  Azaz jelöljük meg mire használjuk az adatot, pl foglalkoztatással összefüggésben. Jogalapról lásd a második fejezetet.
- Ha jogos érdek alapján történik az adatkezelés, akkor ennek az érdeknek a megjelölése.
  A jogos érdekről a jogalapoknál beszélünk bővebben.
- A személyes adatok címzettjeit (vagy azok kategóriáit), ha azt valakinek továbbítjuk
  Például ha egy könyvelő iroda végzi a bérszámfejtést, akkor részére a foglalkoztatással kapcsolatos adatokat továbbítjuk.
- Harmadik országba vagy nemzetközi szervezetnek történő adattovábbítás ténye és címzettjei.
  Erről korábban beszéltünk a munkafüzetben.

A fentiek a kötelező elemei a tájékoztatásnak, ezen felül ajánlottak az alábbiak is, különösen azért, mert a következő részben tárgyalt *hozzáférési jog* esetén egyébként is tájékoztatnunk kell az adat alanyt ezekről.

- Tájékoztatás az érintett azon jogáról, hogy kérelmezheti az adatkezelőtől a rá vonatkozó személyes adatokhoz való hozzáférést, azok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen, valamint az érintett adathordozhatósághoz való jogáról.
  Ezt megtehetjük egyszerű hivatkozással a GDPR cikkelyekre, például *további információért olvassa el a GDPR 13-19. cikkelyeit.*
- Adatkezeléshez kapcsolódó jogok kapcsán, hova küldheti kérését.
- Ha hozzájárulás alapján kezeljük az adatait, akkor a hozzájárulás visszavonásának lehetőségéről és módjáról.
- Az érintett személyes adatok kategóriái.
  A kategóriákat nem határozza meg rendelet, helyette az adatok általunk meghatározott közérthető besorolásáról van szó, például foglalkoztatás céljából „elérhetőségek” kezelése.
- Adott esetben a személyes adatok tárolásának tervezett időtartama, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjai.
  Például a számlán szereplő név, cím tárolása a számviteli törvénynek megfelelő időtartamig fog történni.
- A valamely felügyeleti hatósághoz címzett panasz benyújtásának joga.
- Ha az adatokat nem az érintettől gyűjtötték, a forrásukra vonatkozó minden elérhető információ.

Írjunk a fenti pontoknak megfelelő *adatvédelmi tájékoztatót*.

Az adatkezelő kiléte és elérhetőségei	
Ha van adatvédelmi tisztviselő, az ő elérhetőségét	
A személyes adatok tervezett kezelésének célja és jogalapja	
Jogos érdek alapján történő adatkezelés	
A személyes adatok címzettjei	

Harmadik országba vagy nemzetközi szervezetnek történő adattovábbítás	
Tájékoztatás a jogokról	*Az adat alanya kérelmezheti az adatkezelőtől a rá vonatkozó személyes adatokhoz való hozzáférést, azok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen, valamint az érintett adathordozhatósághoz való jogáról. További információért olvassa el a GDPR 13-19. cikkelyeit.*
Hova küldheti a személyes adatkezelési kérdéseit és kéréseit	
Hozzájárulás visszavonásának módja	
Az érintett személyes adatok kategóriái	
Adott esetben a személyes adatok tárolásának tervezett időtartama, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjai.	
A valamely felügyeleti hatósághoz címzett panasz benyújtásának joga.	*Ha az adatkezeléssel kapcsolatban panaszt szeretne benyújtani az alábbi helyen teheti meg:* *Nemzeti Adatvédelmi és Információszabadság Hatóság* *H-1125 Budapest, Szilágyi Erzsébet fasor 22/c* *Tel.: +36 (1) 391-1400* *ugyfelszolgalat@naih.hu*

III/b. Hozzáférési jog

Az érintett jogosult arra, hogy az adatkezelőtől visszajelzést kapjon arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e. Ha igen, jogosult továbbá arra, hogy a személyes adatokhoz és az lejjebb olvasható információkhoz hozzáférést kapjon.

Ez sok tekintetben hasonló az előző részben tárgyalt rendelkezésre bocsátandó információkhoz, de azt az adatkezelés kezdetekor tesszük elérhetővé az adat alanynak, míg ezeket az adatokat, külön az ő kérésére állítjuk össze. Ahogy ezt említettük, ez lehet eseti válasz a megkeresésre, vagy egy automatizált folyamat, amit például egy weboldalon regisztrált felhasználó, egy menüpont segítségével elérhet.

A hozzáférési jog gyakorlása során az előző részben tárgyalt összes információt rendelkezésre kell bocsátani, az adatkezelési célokról, elérhetőségekről, jogokról. (Ezt már jó esetben megfogalmaztunk az *adatvédelmi tájékoztatóban*.)

Ezen felül, hozzáférést kell adnunk az adatkezelés tárgyát képező személyes adatok másolatához. Azaz a jogot érvényesítő ember számára világossá tesszük mit tárolunk róla. Például nevét és címét és hogy mit vett, ha vásárolt tőlünk valamit. Ha a kérelmet elektronikus úton nyújtották be, akkor ezt könnyen olvasható elektronikus módon bocsátjuk rendelkezésre, például weboldalon vagy PDF dokumentumban.

Természetesen az adatok összegyűjtése, ha nem automatizált módon történik, időigényes lehet. A rendelet alapvetően azt írja elő, hogy ezt a szolgáltatást ingyenesen kell biztosítani, de ha a költségek indokolhatóak akár a komplexitás vagy egyszerűen csak az ismétlődő adatigénylés miatt, akár díjat is számíthatunk fel.

Végül figyeljünk rá, hogy a személyes adatokat annak adjuk ki, aki valóban az adat tulajdonos. Egy weboldal esetén az elektronikus azonosítás elég lehet (korábbi felhasználónév / jelszó regisztráció), míg mondjuk egy foglalkoztatással összefüggő adatkezelés esetén elvárhatjuk azt, hogy az igénylő hitelt érdemlően bizonyítsa személyazonosságát.

Gyakorlati javaslat: Az előző pontban elkészített *adatvédelmi tájékoztatót* azonnal csatolhatjuk válaszunkhoz. Ezen kívül gondoljuk át, hogy hol, milyen személyes adatokat tárolunk, írjuk fel magunknak, hogy a hozzáférési jog gyakorlása során, honnan kell ezeket összeszednünk. Nagyobb adathalmaz esetében ebben nagy segítségünkre lehet egy adatleltár (lásd később a munkafüzetben).

III/c. Helyesbítéshez való jog

Az érintett jogosult arra, hogy kérésére az adatkezelő indokolatlan késedelem nélkül helyesbítse a rá vonatkozó pontatlan személyes adatokat. Például, ha valaki észreveszi, hogy pontatlan cím szerepel a nyilvántartásunkban, kérheti annak korrekcióját.

Hasonlóan a hozzáférési joghoz, nagy léptékű rendszer esetén indokolt lehet ezt automatizálni, míg egyéb esetekben elég, ha valaki ezt manuális teszi meg.

III/d. Törléshez való jog

A rendelet alapján, amikor adatot kezelünk, annak mindig szilárd jogalapja van. Egyúttal azt is kéri a rendelet, hogy csak a meghatározott céllal és ideig tartsuk meg az adatokat. Ha ennek megfelelünk, akkor adat törlésről tulajdonképpen nem beszélhetünk, hisz szilárd indokunk van, ami miatt az nem törölhető. Ennek ellenére tekintsük gyorsan át, hogy működik ez a gyakorlatban.

Az érintettek kérhetik a róluk szóló adatok törlését, de azt csak abban az esetben kell megtennünk, ha az alábbi indokok valamelyike fennáll:

- A személyes adatokra már nincs szükség abból a célból, amelyből azokat gyűjtötték vagy kezelték.
- Ha hozzájárulás alapján kezeltük az adatot, az érintett visszavonja a hozzájárulását.
  Az adatok jelentős részét nem hozzájárulás alapján kezeljük, hanem például szerződés teljesítéséhez vagy jogi megfeleléshez. Ezzel kapcsolatban nem lehet hozzájárulást visszavonni. Ha hozzájárulás alapján kezeltük is az adatokat, a hozzájárulás megszűnésével még mindig lehet más jogalap, például jogi előírás ami miatt az adat nem törölhető.
- Az érintett tiltakozik az adatkezelés ellen, mivel azokat közvetlen üzletszerzés céljából használják (direct marketing) vagy más sajátos indok miatt, ami erősebb mint az adatkezelő indoka az adatkezelés folytatása mellett.
  A sajátos indok nem különösebben definiált a rendeletben, lehet bármilyen személyes helyzettel kapcsolatos ok, ami miatt erre a döntésre jut az adat alany. Ha az adatkezelő úgy dönt, hogy nem törli az adatot, akkor bizonyítania kell, hogy a törlés jogos okokból nem történt meg.
- Az adatokat jogellenesen kezelik.
- Jogi kötelezettség miatt törölni kell azokat.

A rendelet a törlés kapcsán, amennyiben valamelyik fenti feltétel helytálló, az adatkezelő oldalán ésszerűen elvárható mennyiségű erőfeszítést feltételez. Ha az adatok tárolásának jellege ezt különösképpen megnehezíti, akkor a törléstől eltekinthetünk, de ezt alaposan indokolnunk kell.

Továbbá figyelnünk kell arra, hogy ha az adatokat továbbadtuk, akkor a további adatfeldolgozókat is – ésszerű kereteken belül – informálnunk kell az adattörlési kérelemről.

A kisvállalkozások esetén gyakran előfordul, hogy az adatokat eleve csak jogi megfelelés keretein belül tároljuk, például a vevő elérhetősége vásárlás és garanciális ügyintézés esetén, számlainformációk, stb. Ha kizárólag ilyen jogalapokat azonosítunk az adatkezelésnél, a törlésről semmilyen esetben nem eshet szó, így külön ezzel nem kell foglalkoznunk, esetleg csak a vevő informálásával arról, hogy nem lehetséges a törlés.

Van-e olyan személyes adat a rendszerünkben, amit kérésre törölhetünk. Ha nincs, akkor az *adatvédelmi tájékoztatóban* ezt rögzítsük.	IGEN	NEM
Ha vannak jogilag és üzletileg törölhető adatok, akkor azok tárolása hol történik, és hogyan tudjuk őket egyszerűen törölni.		

III/e. Adatkezelés korlátozásához való jog

Előfordulhat, hogy az adat alanya ellene van az adatkezelésnek, de nem azt szeretné, hogy eltávolítsuk a rendszerből, hanem hogy ne kezeljük az adatait. Ez KKVék esetében rendkívüli ritka lesz, de tekintsük át, hogy miről is van szó.

- Az adatok pontatlanok, amíg ez nincs javítva, azokat ne használjuk.
- Az adatkezelés jogellenes, az adat alany azt kéri hogy ne használják, ám ne is töröljék azokat. (Egy esetleges későbbi jogvita miatt szeretné, ha megtartanánk.)
- Az adatkezelő már törölné az adatokat, de arra az adat alanynak szüksége van. (Például egy biztonsági kamera felvétele, amire valakinek később szüksége lesz jogi eljárásban.)
- Tiltakozott az adatkezelés ellen (lásd később).

A jogérvényesítés itt bonyolult lehet. Általában beválhat, ha a rendszereinkből kimásoljuk az érintett adatokat és onnan el is távolítjuk azokat, így nem történhet semmilyen adatkezelés velük kapcsolatban, de a személyes adatok továbbra is elérhetőek. Például lemásoljuk a biztonsági kamera felvételét és azt eltároljuk, amíg az adat alanya kéri.

III/f. Adathordozáshoz való jog

Kérheti az adat alany, hogy a róla meglévő információinkat, gépi feldolgozásra alkalmas formában adjuk át, hogy ő azt más szolgáltatóval, más rendszeren tudja használni. Ennek a jognak akkor van értelme, ha valami szisztematikus adathalmazt (elektronikusan) tárolunk a személyről.

Az olyan adatok, amikből egy van, például az alany neve, címe, nem igazán szisztematikus, ezeknek az átadása egy sima lista. De könnyen lehet, hogy vannak szisztematikus, táblázat szerű adataink is, például bérszámfejtésnél az elmúlt évek bérhez kapcsolódó adati (mikor mennyit keresett, stb).

Elvileg az ilyen adatokat, gépi olvasásra alkalmas formátumban adjuk át, ilyen például az XML, JSON vagy CSV. CSV formátumot Excelből bármikor tudunk exportálni. Ha el tudjuk érni, hogy az adatokat egy Excel jellegű fájlba látjuk, akkor nyert ügyünk van. Félő, hogy nem minden szoftveres nyilvántartás kompatibilis jelen pillanatban ezzel a kívánalommal, például nem minden könyvelési programból lehet ilyen adatokat könnyedén exportálni.

Gyakorlatban, tekintettel a valószínűsíthetően ritka megkereséseknek, a rendelkezésre álló egy hónapos határidőnek, azt javasoljuk, hogy átlagos esetekben erre külön ne készüljön egy KKV. Ha a cég profiljában nagy mennyiségű adatot kezel, ahol az ilyen megkeresés gyakori lehet (például híváslista egy telefonszolgáltatásnál), akkor természetesen erre automatizált eszközöket érdemes építeni.

III/g. Tiltakozáshoz való jog

Az utolsó jog amivel foglalkoznunk kell a tiltakozáshoz kapcsolódik. Fontos esetei:

- Ha a vállalkozás *jogos érdeke* alapján kezeljük az adatokat, ez ellen tiltakozhat az adat alany. Ha nincsenek elsőbbséget élvező, kényszerítő erejű jog alapok, akkor nem kezelhetjük tovább az adatot. A *jogos érdekről* a jogoknál a második fejezetben már írtunk.
- Közvetlen üzletszerzés esetén (direct marketing), az adat alany szeretne kikerülni a rendszerből. Ez esetben a megkeresésekkel fel kell hagynunk.

III/h. Összefoglalás a GDPR jogokról

Jópár oldalon foglalkoztunk a kapcsolódó jogokról, amit valamilyen módon biztosítanunk kell. De a megfelelés sok esetben nem ilyen bonyolult. A fentebb vázolt *adatvédelmi tájékoztatót* érdemes megírni és elérhetővé tenni. Ha ezt a dolgozók számára készítjük, akkor kifüggesztjük a faliújságra vagy mellékeljük a munkavállalói szerződés mellé. Ha a vevőink számára, akkor honlapunkon közzétehetjük.

Amikor valaki valamely jogát érvényesíteni akarja, akkor az kényelmetlen adminisztrációs terhet jelenthet, de nem teljesíthetetlen. Ha a fenti jogokat alapvetően értjük és van elképzelésünk róla, hogy mit tegyünk ha valaki kapcsolódó kéréssel az ajtónkon kopogtat, nem kerülhetünk bajba.

A kicsit nagyobb vállalkozásoknak hatékony GDPR megfelelési demonstráció lehet, ha a GDPR jogok elérhetőségével kapcsolatban belső folyamatot hoznak létre és azt dokumentálják. Leírják néhány mondatban, hogy mi fog történni például, ha valaki kikéri az adatait. De az ilyen dokumentumok megírása egyáltalán nem kötelező.

IV. Technikai és szervezési intézkedések

Az adatvédelem korunkra elsősorban (de nem kizárólag) technikai kérdés. Ebben a fejezetben egy egyszerű ellenőrzőlistát mutatunk be, amelyen egyszerűen bejelölhető, hogy a vállalkozás mely intézkedéseket tette eddig meg. A rendelet nem ír elő kifejezett technológiákat amiket alkalmaznunk kell, csupán azt mondja, hogy az elérhető megoldások közül a kockázatoknak megfelelőt válasszunk.

A lista természetesen nem teljes és kifejezetten a KKVékra van szabva, egy nagyvállalat lehetőségei ennél jóval tágabbak.

	Zárható iratszekrény		Biztonsági őr
	Jelszóval védett WiFi (WPA2-PSK vagy jobb titkosítással)		Iratmegsemmisítő használata
	Felhasználónév + jelszóval védett számítógépek		Csak definiált felhasználói csoport által elérhető adattároló
	Tűzfal a vállalati hálózat és az internet között		Titkosított adattároló
	Fizikai beléptető rendszer		Elzárt szerverek
	IT biztonsági oktatás		Hozzáférés kezelés (pl. Active Directory)
	Vírusirtók		Auditálás
	Adattárolási szabályzat		Biztonsági másolat (backup)
	Jelszóval vagy biometrikus azonosítóval védett mobil eszközök		Egyéb:
	Egyéb:		Egyéb:

V. Egyéb kapcsolódó iratok

Vannak egyéb dokumentációk, amiket egyszerűségük miatt esetenként érdemes elkészítenünk. Ezek nem kötelezőek, egy bonyolultabb adatkezelést megvalósító vállalkozásnak ajánlott lehet.

V/a. Adat leltár

Az adat leltár egy lista az általunk kezelt személyes adatokról és a hozzá kapcsolódó gyakorlatunkról. Ennek rendeletileg definiált formai követelménye nincs, a közkézen forgó GDPR leltárminták egyéb tanúsítási eljárásokból kölcsönöznek mintákat. Az előadáson bemutatott *egyszerű adatleltár* és az ICO által közzétett *adatkezelési tevékenység nyilvántartása* is díjmentesen elérhető az alábbi honlapon, egyéb hasznos dokumentumokkal, kitöltési útmutatóval:

- **zenit-services.com/dokumentumok.html**

V/b. Adatkezelési incidens nyilvántartás

A rendelet előírja, hogy az illetékes hatóságot (NAIH) az esetek többségében értesíteni kell az incidensekről, továbbá ezekről az incidensekről nyilvántartást kell vezetnünk. Ilyen incidens lehet, ha az adatokat ellopják, azokat elveszítjük vagy megsemmisülnek.

Ezek nyilvánvalóan ritka események a KKV életében, de a hatóság kérheti az adatkezelési incidens nyilvántartásunkat. Ez nagy valószínűséggel incidensek híján egy üres lap lesz, a megfelelő fejléccel. A nyilvántartás elemei:

- Dátum, időpont
- Incidens leírása
- Érintettek csoportja és száma
- Valószínűsíthető következmények az érintettekre nézve
- Hatósági tájékoztatás történt-e / mikor
- Az adat alanyok tájékoztatása szükséges-e, ha igen, mikor milyen formában történt ez meg
- A hasonló incidens jövőben elkerüléséhez tett intézkedések

A fenti tényeket rögzítő excel fájl tökéletesen alkalmas lehet ilyen nyilvántartásra. Ehhez találhat mintát az alábbi honlapon:

- **zenit-services.com/dokumentumok.html**

VI. Néhány gyakori eset

VI/a. Foglalkoztatáshoz kapcsolódó adatkezelés

Ha más nem is, de a foglalkoztatás kapcsán biztos van személyes adatokat érintő adatkezelésünk. Ezen adatok tekintetében mi vagyunk az adatkezelők.

A foglalkoztatás munkaszerződés alapján történik, így a jogalapja az adatkezelésnek is ez. A kapcsolódó papír alapú és elektronikus dokumentumokat valamilyen minimális védelemmel lássuk el, az iratokat helyezzük zárható szekrénybe, a fájlok legyenek felhasználónév és jelszó által védett számítógépen vagy hálózati meghajtón.

Harmadik felt is bevonunk az adatkezelésbe, ha nem házon belül, hanem könyvelőcéggel végeztetjük a bérszámfejtést. Ilyen esetben a könyvelő cég adatfeldolgozó:

- A könyvelő cég, a mi írásos utasításunk alapján kezelheti csak az adatokat. Az utasításunkban meghatározzuk, hogy milyen adatokat kapnak meg (vagy férnek hozzá) és azokat milyen céllal kezelhetik.
- Ha adatfeldolgozót alkalmazunk, meg kell bizonyosodnunk arról, hogy ő is GDPR előírásoknak megfelelően dolgozik. Ez ügyben elég, ha a könyvelő cég írásos garanciát vállal, miszerint a megfelelő belső szabályok és adatvédelmi intézkedések náluk ehhez megvannak.

A dolgozókat tájékoztatnunk kell az adatkezelés tényéről. Ez lényegében a korábban már tárgyalt adatvédelmi tájékoztató, a foglalkoztatásra vetítve.

A foglalkoztatáshoz kapcsolódó dokumentumokat, mint *maradandó értékű iratokat*, meg kell őrizni, tulajdonképpen örökre; a gyakorlatban amíg elévülnek. Az ilyen iratokra például a munkavállalónak, nyugdíj kapcsán később szüksége lehet.

VI/b. Számlák

Az adatvédelmi rendeletnél a helyi törvénykezések mindig erősebbek, ilyen például a számviteli törvény. Ennél fogva, bár a számlák tartalmaznak személyes jellegű információkat, azoknak az adatait nem törölhetjük az előírt 8+1 év előtt, még ha valaki kifejezetten kéri is ezt.

Ellenben az idő lejárta után, mivel azok személyes információkat tartalmaznak és további szükségünk nincs rá, az adat minimalizálás értelmében selejteznünk kell.

VI/c. Álláshirdetés

Ha új pozíciót írunk ki a vállalkozásunknál, van néhány egyszerű dolog amire figyelnünk kell:

- Bár az önéletrajz személyes adat, az álláshirdetés kapcsán nekünk küldött önéletrajzok kezelése a cég jogos érdekkörébe tartozik, így ahhoz külön nem kell engedélyt kérnünk.
- Ellenben az önéletrajzokat nem tárolhatjuk örökké. Ha a meghirdetett állást betöltötték, a beérkezett önéletrajzokat törölnünk kell, mivel az adatkezelés célja teljesült. Azonban az állás betöltése után potenciálisan előfordulhat diszkriminációval kapcsolatos panasz. Ilyen panaszok ellen, a jelentkezők adatait bizonyítékként felhasználhatjuk. A törvényi határidő hátrányos megkülönböztetés kapcsán indult eljárásnál 3 év. Ezért az önéletrajzokat, ebből a célból további, 3 évig érdekünkben áll tárolni és ezt erre hivatkozva meg is tehetjük.
- Ha szeretnék az önéletrajzot hosszabb ideig megtartani és valamikor a jövőben újra elbírálni a jelentkezők adatait egy új álláslehetőség kapcsán, erre csak a hozzájárulásukkal van lehetőségünk. Ezt kérhetjük például e-mailben is. Vegyük figyelembe, hogy általános szabályként az önéletrajz 3 év után elévültnek tekintendő.
- Habár az önéletrajz kezelése jogos érdek alapján történik, a transzparencia elve alapján, ez ügyben is érdemes közzé tenni adatvédelmi tájékoztatót, amely hasonlóan a már tárgyalt gyakorlathoz, leírja a toborzás során történő adatkezelést.

VI/d. Céges e-mail fiók

Mégha egy e-mai fiók alapvetően üzleti céllal készül el, a dolgozó szándéka ellenére is kerülhet bele személyes információ, ennél fogva az e-mail fiókok mindig privát adatként kezeljük. A fiók tulajdonosán kívül, más nem olvashatja azokat.

Ha a dolgozó elhagyja a céget, egyetlen dolgunk van, az e-mail fiókot minden tartalmával együtt törölni.

VI/e. Céges eszközök

A dolgozónak esetenként mindenféle eszközöket adunk (telefon, pc, laptop, tablet, stb), amikre a mindennapi használat során személyes információ kerülhet. Bár belső szabályzattal a munkától eltérő felhasználást tilthatjuk, ez az elvárás általában nem életszerű. Ennél fogva, ha a dolgozó elhagyja a céget, a személyes eszközén található adatokat mérlegelés és betekintés nélkül töröljük.

VI/f. Felhő (cloud) szolgáltatások

Nagyon sok cég használ különféle felhő szolgáltatásokat, mint például Google Mail, Amazon EC2, stb. Az esetek jelentős részében kerülnek személyes adatok az ilyen szolgáltatóhoz (például amikor e-mailt küldünk Gmail-en keresztül), ilyenkor ők adatfeldolgozónak számítanak. A komolyabb szolgáltatók erre fel vannak készülve, egyrészt vállalják a GDPR garanciákat, másrészt a honlapjukon alá lehet írni valamilyen fajta adatkezelési megbízást. Ez általában elégséges, kisebb szolgáltatóknál érdemes közelről szemügyre venni a szerződéseket.

VII. Záró gondolatok

Az adatvédelmi rendelet által támasztott követelmények egyszerre bonyolultak és egyszerűek is. Alapvetően azt kéri, hogy *tisztességes adatkezelést* valósítsunk meg, *élhessenek az emberek az adathoz kapcsolódó jogaikkal*, tegyünk *megfelelő technikai és szervezési intézkedéseket* az adatok védelméért, végül pedig, hogy *jelentsük az incidenseket*.

Minden kisvállalkozás életében történik adatkezelés, ha más nem a foglalkoztatás kapcsán, de egy *adatvédelmi tájékoztató*, egy *incidens nyilvántartás* és egy GDPR jogokkal tisztába levő *adatjogok kapcsán elérhető személy* megléte bőségesen elég intézkedés lehet.

Reméljük, hogy előadásunk és munkafüzetünk hozzásegítette az Ön vállalkozását is, hogy közelebb kerüljön a GDPR megfeleléshez.

Az előadás és a munkafüzet a Győr-Moson-Sopron Megyei Kereskedelmi És Iparkamara, és a Zenit Services támogatásával készült.

Honlapunkon, az előadással megegyező szellemiségben elkezdtük kialakítani és folyamatosan bővítjük az adatvédelmi rendelethez kapcsolódó tudnivalókat. Keressen fel minket további információkért és programokért:

- **gymskik.hu**
- **zenit-services.com**