Melyek a GDPR alapelvei és miért hasznos ezeket ismernünk?

Az alapelvek azért vannak, hogy jobban megértsük, miről is szól ez az egész adatvédelmi szabályrendszer, illetve, ha bizonyos előírások értelmezésével gondunk van, akkor az alapelvek azok, amihez visszatérhetünk.

Melyek ezek az alapelvek?

1) „jogszerűség, tisztességes eljárás és átláthatóság elve”: a személyes adatok
kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni.
A személyes adatokat egyrészt mindig úgy kell kezelnünk, hogy megfeleljünk a vonatkozó jogszabály előírásának (például a kisállat útlevélről szóló rendelet előírja, a gazdik milyen adatai kezelhetők, akkor a jogszabály alapján csakis azok), másrészt a kezelés közben tisztességesen kell eljárnunk – azaz például a szerződéses partnereink adatait nem adjuk ki aloevera (vagy bármi más tukmálásával foglalkozó) ügynöknek még akkor sem, ha úgy gondoljuk, az aloevera (vagy bármi más) jót tenne az egészségüknek. A tisztességes és átlátható adatkezelés megkívánja, hogy az adatokat úgy kezeljük, hogy azok nyomon követhetők legyenek és az érintett nem jut arra a sorsra, hogy Trinidad-Tobagóba bejegyzett online kaszinóból kap naponta több visszautasíthatatlannak tűnő ajánlatot a mi slendriánságunk miatt.

2) „célhoz kötöttség elve”: a személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történhet és nem kezelhetők ezekkel a célokkal össze nem egyeztethető módon.
Az adatokat mindig csak meghatározott célból gyűjthetjük – ha ebregiszternek, akkor ebregiszternek, ha kutyaeledel gyártó cégnek marketing célból (cserébe kap a gazdi két zacskó ingyen tápot), akkor abból, de mindig meg kell tudni mondanunk, mi a célunk.
És nemcsak meg kell tudnunk mondani, mi a célunk, hanem a célt nem csereberélhetjük tetszésünk szerint – az ebregiszterbe általunk bejegyzett állattartói adatokat nem használhatjuk fel marketing célra és fordítva.

3) „adattakarékosság elve”: a személyes adatok az adatkezelés céljai szempontjából megfelelőek és relevánsak kell, hogy legyenek és a szükségesre kell korlátozódniuk.
Mindig csak annyi adatot gyűjthetünk, amennyire feltétlen szükségünk van. Amennyiben például jogszabály mondja meg, milyen adatokat kell elkérnünk, akkor szigorúan ragaszkodnunk kell ezekhez az adatokhoz és ha például nem kéri a személyi igazolványszámot, akkor mi sem kérhetjük el. A hozzájárulásos adatkezelésnél nehezebb dolgunk van, mert ott – általában – nem mondja meg jogszabály, milyen adatokban kell gondolkodnunk az adott adatkezelés tekintetében, hanem nekünk kell eldöntenünk, melyek a feltétlen szükséges adatok. Ha például hírlevél szolgáltatást üzemeltetünk, akkor mindenképpen meg kell győződnünk arról, hogy a jelentkező elérte azt a korhatárt, ami felett már nem kell szülői beleegyezés ahhoz, hogy törvényes legyen az adatainak a kezelése. Az egyik módszer például olyan kritérium

kikötése, ami garantálja az adatvédelmi nagykorúságot (például kamarai tagság megkövetelése a hírlevélre
feliratkozáshoz), vagy nyilatkoztathatjuk is abban a tekintetben, hogy a kora már meghaladta a 16 évet. Az ilyen esetekben a születési időpontra rákérdezés nem felesleges, hiszen a hozzájáruló nyilatkozat érvényessége függ attól, hogy arra jogosult adtae.
Azt azonban már nehezen tudnánk indokolni, hogy egy hírlevélre feliratkozáshoz miért is van szükségünk az érintett anyja nevére.
4) „pontosság elve”: a személyes adatoknak pontosnak és szükség esetén naprakésznek kell lenniük és minden észszerű intézkedést meg kell tenni annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatok haladéktalanul törölve vagy helyesbítve legyenek.
Ha adatokat gyűjtünk, akkor azok legyenek pontosak, különben nem biztos, hogy a célnak megfelelően használni is tudjuk azokat. Ha szól a szerződéses partnerünk, hogy megváltozott a számlázási (szállítási) címe, akkor nekünk is módosítani kell az adatainkat, különben nem tudunk szerződésszerűen számlázni (teljesíteni), ha pedig eleve elírtadat került bele a szerződésbe, amint tudomást szerzünk róla, szintén javítanunk kell.
5) „korlátozott tárolhatóság elve”: a személyes adatok tárolásának olyan formában
kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig tegye lehetővé.
Az adatok egy tetemes része nem örökgaranciás, éppen ezért kell időről időre selejteznünk (adatot megsemmisítenünk). Nem azért kell kidobnunk a 10 évvel ezelőtt megszűnt irodatakarítási szerződést, mert nem férünk a szekrényben, hanem azért, mert az adatkezelés célja réges-régen megszűnt: nincs már garancia, a peresítés lehetősége is elévült, sőt már a szerződés alapján készült számlákat sem vizsgálhatja az adóhivatal.
Az selejtezés során gondoskodjunk arról, hogy csak olyan iratot selejtezzünk le jegyzőkönyvileg, amely nálunk volt (iktatókönyvben szerepelt), azaz utólagosan se bizonyítsunk magunkra jogosulatlan adatkezelést. Arra is mindig vigyázzunk, hogy az adatok nyomon követhetősége érdekében tudjunk arra az esetleges érintetti kérdésre válaszolni, miszerint mikor és hogyan szüntettük meg a vele kapcsolatos adatkezelést – például volt munkavállalónk esetében tudjuk teljes magabiztossággal négy évvel a tőlünk kilépése után azt mondani, hogy már csakis azok az adatokat kezeljünk vele kapcsolatban, amelyek megőrzésére jogszabály kötelez minket, a jelenléti íveit meg a kamarai internet használatának ellenőrzésével kapcsolatos dokumentumokat pedig már megsemmisítettük.
Persze vezethetünk feketelistát „velük soha többé az életben nem szerződünk” adatkezelési céllal, ennek az adatkezelésnek a célja azonban már teljesen más, mint az eredeti szerződéses célú volt – ebben az esetben az eredeti szerződést le kell selejteznünk és csak a személyes, az adott személy beazonosítására alkalmas minimális mennyiségű adatot tarthatjuk nyilván a szervezet jogos érdeke alapján. Ebben az esetben érdekmérlegelési tesztet kell végeznünk, amely során bebizonyítjuk, a feketelistánkon szereplő hanyag, dolgozni nem tudó személyt nem akarjuk többet látni az irodánkban, mert már a szimpla jelenléte is kárt okoz a szervezetnek.
6) „integritás és bizalmas jelleg elve”: 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.

A GDPR összetolta a jogszerű adatkezelést az adatbiztonsággal – azaz nemcsak arra kell ügyelnünk, hogy megfelelő, jogszerű célra hivatkozva, időben szavatos és helyes adatokat tartsunk nyilván, hanem arra is, hogy ezek az adatok mindaddig biztonságban legyenek, ameddig nálunk vannak – ha pedig kiderül, hogy erre képtelenek voltunk, akkor bizony előfordulhat, hogy önfeljelentés keretében az adatainkat ért adatvédelmi incidenst be kell jelentenünk a Hatóságnak.
A védelem módját és mértékét mindig nekünk kell eldöntenünk a szervezetünk sajátosságait figyelembe véve – egy kettő fős irodától nem várható el, hogy Fort Knox szintű védelmet biztosítson, ám az adatkezelőnek kutya kötelessége, hogy minimum nehezen megfejthető jelszóval védje az adatbázisát, ne hagyja szanaszét a laptopját, legyen
gyakran biztonsági mentés és az iratokat se vigye ki a huzat az ajtón.

Összegezve az alapelveket:
- személyes adatot kizárólag meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében kezelhetünk,
- az adatkezelésünknek az adatkezelés minden szakaszában meg kell felelnie az adatkezelés céljának, valamint az adatok felvétele és kezelése során tisztességesnek kell lennünk és a vonatkozó jogszabályok szerint kell eljárnunk,
- csak olyan személyes adatot kezelhetünk, amely az adatkezelésünk céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas, valamint csak a cél megvalósulásához szükséges mértékben és ideig kezelhetjük azokat,
- az adatkezelés során biztosítanunk kell az adatok pontosságát, teljességét és - ha az adatkezelés céljára tekintettel szükséges - naprakészségét, valamint
- arról is gondoskodnunk kell, hogy az érintettet csak az adatkezelés céljához szükséges ideig lehessen azonosítani,
- ha pedig már nem tudunk célt rendelni az adatokhoz, az adatkezelést haladéktalanul meg kell szüntetnünk, az adatokat (iratokat, fájlokat) pedig bizonyítható módon meg kell semmisítenünk.