**GDPR**

*Általános adatvédelmi rendelet*

* A GDPR röviden az Európai Unió és a Tanács által elfogadott, a személyes adatok védelméről és az ilyen adatok szabad áramlásáról szóló rendelete, más néven általános adatvédelmi rendelet (General Data Protection Regulation) amelyet **2018. május 25**-étől kell alkalmazni.
* Közvetlen hatállyal rendelkezik, minden tagállamban kötelezően alkalmazandó, ez a rendelet a legfontosabb szabályanyag a személyes adatok kezelése és védelme tekintetében.
* A jogsértés típusától, illetve a GDPR-ban található szabályoktól függ az adatvédelmi bírság mértéke. A rendelet szabályai szerint maximálisan 20 millió eurót lehet kivetni, vagy az adott vállalat előző pénzügyi évének teljes éves világpiaci forgalmának mintegy 4%-át teheti ki az összeg, a kettő közül azonban a magasabbat kell kiszabni. A tagállamoknak jogában áll adatvédelmi jogsértések esetén további büntetőjogi szankciókat kiszabni.
* A GDPR alapelvek megerősítik a személyes adatok kezelésével érintett személyek jogainak biztonságát, ugyanakkor növeli az adatkezelő cégekbe vetett vásárlói, fogyasztói bizalmat, hiszen a felhasználók, adatalanyok biztosak lehetnek benne, hogy nem történik visszaélés személyes adataikkal kapcsolatban. Ha egy vállalkozásról, cégről bebizonyosodik, hogy a személyes adatok kezelése, feldolgozása mindenben megfelel a jogszabályoknak, az növeli a cég, vállalkozás üzleti hírnevét, megbízhatóságát, üzleti kapcsolatait. Tény, hogy a GDPR felkészülés plusz energiát vesz el és költségeket is jelent a cégnek, de úgy gondoljuk, hogy ez feltétlenül tekinthető a cég értéknövelő, hosszú távú beruházásának.
* Magyarországon a NAIH (Nemzeti Adatvédelmi és Információszabadság Hatóság) felel majd a GDPR betartatásáért, ellenőrzéseket folytathat le, az adatvédelmi szabályok megsértőit szankcionálhatja.
* Az adatkezelés magában foglal szinte minden, a személyes adatokon végzett cselekményt, így azok felvételét, gyűjtését, tárolását, különböző célokra történő felhasználását, továbbítását, módosítását, hogy csak néhány adatkezelési műveletet említsünk. Az ezt végző személy **az Adatkezelő**. Az, aki az adatkezelő megbízásából és nevében személyes adatokkal dolgozik, az **Adatfeldolgozó**.
**Adatkezelő** – *„az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza; ha az adatkezelés céljait és eszközeit az uniós vagy a tagállami jog határozza meg, az adatkezelőt vagy az adatkezelő kijelölésére vonatkozó különös szempontokat az uniós vagy a tagállami jog is meghatározhatja”.*

**Adatfeldolgozó** – „*az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel”.*

**Adatkezelési alapelvek:**

1. „*jogszerűség, tisztességes eljárás és átláthatóság”*

Tehát az érintett számára transzparens módon kell eljárni. Mit jelent itt az átláthatóság? Ez azt jelenti, hogy az érintett számára az adatfeldolgozás minden egyes szakasza (gyűjtés, törlés, továbbítás stb.) ismert, és minden fél (hatóság, adatkezelő és érintett) tudatában van a személyes adatokra vonatkozó információnak (ki, milyen célból, hol, milyen jogalappal tárolja, hozzáférést hogyan védi, mikor törli etc.).

1. „*célhoz kötöttség”*

Az adatgyűjtés jól meghatározott, jogszerű célból történhet, a kitűzött célokkal össze nem egyeztethető módon nem lehet ezeket kezelni.

1. „*adattakarékosság” vagy „adatminimalizálás”*

Csakis az igazán szükséges adatokat tároljuk. Ne az férjen hozzá a személyes adatokhoz, akinek erre jogosultsága van, hanem az, aki a vállalaton belül kimondottan ezzel foglalkozik, és az adatkezelésre feltétlenül szüksége van.

1. „*pontosság”*

Az adatoknak a valósággal megegyezőnek kell lennie, ellenkező esetben mindent meg kell tenni annak érdekében, hogy az adatokat korrigálják vagy töröljék.

1. „*korlátozott tárolhatóság”*

Az adatok addig legyenek elérhetőek, tehát az érintetteket csak addig lehessen beazonosítani, míg a személyes adatok kezelésének célját el nem értük.

1. „*integritás és bizalmas jelleg”*

A személyes adatok tárolását oly módon kell végrehajtani, hogy védve legyenek jogosulatlan vagy jogellenes kezeléstől, illetve ne lehessen elveszteni, megsemmisíteni vagy károsítani.

1. „*elszámoltathatóság”*

A GDPR nagy újítása az elszámoltathatóság bevezetése. Az adatkezelőnek a fentebb részletezett pontoknak köteles megfelelni, és megfelelőségét dokumentumokkal alátámasztani. Tehát itt fordított bizonyítási kényszer áll fenn, azaz nem az adatvédelmi hatóságnak, üzleti partnernek, érintettnek kell bizonyítania, hogy jogszerűtlen kezelés történt, hanem a vállalkozásoknak kell az egyes adatkezelésükről dokumentumot vezetni, melyet kötelesek az adatvédelmi hatóság vagy a beszállító kérésére átadni. Így bizonyítja a vállalat az adatvédelmi megfelelést. A hatóságok külön figyelmet fordítanak az adatkezelés jogalapjára és céljára, valamint a címzettek körére, illetve az alkalmazott védelmi (technikai és szervezési) intézkedésekre. Az elszámolhatóság elve a gyakorlatban úgy teljesül, hogy egy aktában átnyújtjuk az ügyfelek, adatvédelmi hatóság és az érintettek részére mindazon jegyzőkönyvet, nyilvántartást és egyéb dokumentumokat, amelyek bizonyítják jogszerű eljárásunkat.

Az adatkezelés elvégzéséhez szükség van megfelelő jogalapra, amennyiben ez nem áll rendelkezésre, el sem lehet kezdeni a tevékenységet. Amennyiben a tevékenység közben szüntetik meg a jogalapot, akkor azonnal be kell fejezni az adatkezelést is, és törölni kell a személyes adatokat vagy anonimmá kell tenni.

A személyes adatokat akkor kezelik jogszerűen, ha a következők közül legalább az egyik teljesül:

* 1. az érintett megadta hozzájárulását ahhoz, hogy a személyes adatait kezeljék;
	2. az adatkezelés olyan szerződéshez szükséges, melyben az egyik fél az érintett;
	3. az adatkezelés ahhoz szükséges, hogy az adatkezelőre vonatkozó jogi kötelezettségek teljesüljenek;
	4. az adatkezelés ahhoz szükséges, hogy az érintett létfontosságú érdekeinek védelmét biztosítsa;
	5. az adatkezelés ahhoz szükséges, hogy közérdekű feladatokat hajtsanak végre;
	6. harmadik fél vagy az adatkezelő jogos érdeke érvényesítéséhez szükséges.

Amennyiben több jogalap áll rendelkezésünkre, választani kell közülük. A választás komoly hatással lehet az adatkezelésre. Például, a hozzájárulás bármikor visszavonható, a szerződés viszont nem.

Többlet adminisztrációval járhat az az eset, amikor az adatkezelő jogos érdekre hivatkozva kezel személyes adatot. Ilyenkor érdekmérlegelési tesztet kell készíteni. Ezzel meg lehet állapítani, hogy a cél jogszerű-e (jogszerűség-vizsgálat). Amennyiben igen, akkor következőként meg kell állapítani, hogy tényleg szükség van-e az adatkezeléshez a cél eléréséhez (szükségesség-vizsgálat). Abban az esetben, ha jelentős anyagi ráfordítás nélkül is elérhető a célunk az adatkezelés nélkül, akkor természetesen nem szükséges az adatkezelés, tehát már nem jogszerű az adatkezelés jogos érdekekre hivatkozva. Azonban, ha jogszerű az adatkezelés célja, és az ehhez szükséges adatkezelés is, meg kell vizsgálni, hogy a jogi érdekünk milyen arányban áll a személyes adat védelméhez kapcsolódó joggal (arányosság-vizsgálat). Ha a vállalkozás választása a jogos érdek jogalapja, akkor a legnagyobb mértékű szabadságot választja az adatkezelő számára, ugyanis nem köti a szerződés érvényessége, hatályossága az érintett hozzájárulása, a jogszabályi felhatalmazás megléte, azonban ez jár a legnagyobb adminisztratív kötelezettséggel. Az egyes vizsgálatok több tíz oldal mennyiségű kérdéssel és azok kiértékelésével hajthatóak végre. Ennek ellenére igen valószínű, hogy ez lesz az egyik legnépszerűbb jogalap, ezért érdemes tájékozódni ennek részletszabályozásáról is, illetve megismerkedni ennek piaci gyakorlatával.

Hozzájáruláson alapuló jogalap alkalmával az adatkezelőnek tudnia kell bizonyítani, hogy az érintett hozzájárulását szabadon adta meg, és jól el kell különíteni a hozzájárulási kérelmet a többi adattól.

A rendelet külön kitér arra, hogy mikor megengedett a személyes adatoknak az eredeti céltól eltérő más célból történő kezelése.

A rendelet meghatározza a szerződés kötelező elemeit, mely az adatkezelők és az adatfeldolgozók között köttetik. Az adatfeldolgozóknak újbóli kötelezettségeket kell teljesíteniük. Az adatkezelők csak olyan adatfeldolgozókat kérhetnek fel, akik teljesíteni tudják a GDPR-nak megfelelő szervezési és technikai intézkedéseket.

A szerződésnek minimum a következőkre kell kitérni:

1. Az adatfeldolgozó kizárólag olyan utasításokat hajthat végre, amelyek írásban rögzítettek.
2. Titoktartás kötelezi a személyes adatok kezelésével foglalkozó munkavállalókat.
3. Az adatbiztonság garantálása érdekében az adatfeldolgozó végrehajtja a szervezési és technikai intézkedéseket.
4. Az adatfeldolgozó segíti az adatkezelőt abban, hogy teljesítse kötelezettségeit.
5. Az adatfeldolgozó az adatkezelő döntése alapján minden személyes adatot visszajuttat az adatkezelőnek vagy töröl, törli a meglévő másolatokat, egy kivétellel, ha a tagállami vagy az uniós jog az adatok tárolását írja elő.
6. Az adatfeldolgozó elősegíti és lehetővé teszi az adatkezelő által vagy az általa megbízott ellenőr segítségével végzett auditokat, helyszíni vizsgálatokat.

Amennyiben az adatfeldolgozó további adatfeldolgozó segítségét veszi igénybe, úgy őrá ugyanazok a kötelezettségek vonatkoznak, mint amelyek eredetileg a szerződés által létrejöttek az adatfeldolgozó és az adatkezelő között.

* Uniós rendelet lévén a GDPR az EU-hoz valamilyen oknál fogva kapcsolódó adatkezelésekre állapít meg rendelkezéseket. Így alkalmazni kell a GDPR-t, ha Ön, vagy a vállalkozása/cége tevékenységét az Unió területén fejti ki, és az adatkezelés e tevékenységével összefüggésben valósul meg.
* Alkalmazandó azokra az adatkezelésekre, adatfeldolgozási műveletekre is, amelyeket az Unióban tevékenységi hellyel nem rendelkező adatkezelő vagy adatfeldolgozó végez, ám áruknak vagy szolgáltatásoknak az Unióban tartózkodó érintettek számára történő nyújtásához kapcsolódnak, vagy az érintettek Unió területén belül tanúsított viselkedésének megfigyeléséhez kapcsolódnak.
* Megszűnik a most működő, a NAIH által vezetett adatvédelmi nyilvántartás, **az egyes adatkezeléseket nem kell bejelenteni.
Bejelentési kötelezettség keletkezik viszont** az adatkezelő oldalán ún. adatvédelmi incidensek, azaz személyes adatokkal kapcsolatos jogsértések esetén, az adatkezelő általi tudomásszerzést követően haladéktalanul, de legkésőbb 72 órán belül.
* A GDPR szerint az adatkezeléssel érintett személyeknek az alábbi jogaik vannak:
1. **Tájékoztatáshoz való jog:**
	* A természetes személy jogosult személyes adatáról átlátható, tömör, könnyen hozzáférhető és közérthető tájékoztatást kapni, különösen az alábbiakról.
	* az adatkezelő elérhetősége és kiléte
	* az adatvédelmi tisztviselő elérhetőségei
	* az adatkezelés jogalapja, illetve a személyes adatok tervezett kezelésének célja
	* az adatkezelés okai
	* a személyes adatok címzettjei
	* az EU-n kívülre történő adattovábbítás esetén a biztosított garanciák
	* az adatkezelés tervezett időtartama
	* az érintett azon jogairól szóló dokumentum, amely részletezi, hogy az érintett kérelmezheti az adatkezelőtől az érintettre vonatkozó személyes adatokhoz való hozzáférést, valamint azok helyesbítését, kezelésének korlátozását vagy törlését
	* tiltakozhat a személyes adatok kezelése ellen,
	* tájékozódhat az érintett adathordozhatósághoz való jogáról,
	* rendelkezik a felügyeleti hatósághoz címzett panasz benyújtásának jogával,
	* arról, hogy a szerződés megkötésének előfeltétele-e az adatainak megadása, illetve arról, hogy milyen lehetséges következményekkel járhat az adatszolgáltatás megtagadása vagy elmaradása,
	* legvégül az automatizált döntésekről, beleértve a profilalkotást is.
	* Amennyiben az adatkezelő az eredeti céltól eltérő vagy további célt fogalmaz meg, a tevékenységek megkezdése előtt tájékoztatni kell erről az érintettet. Abban az esetben, ha a személyes adatokat nem közvetlenül az érintettől szerezték meg, erről tájékoztatni kell az érintettet, meg kell adni az adatok forrását, akkor is, ha az adatok nyilvánosan hozzáférhetőek.
2. **Hozzáféréshez való jog:**
* Az adatkezelő köteles másolatot készíteni a személyes adatokról az érintett számára, mely történhet videofelvétel, feljegyzés stb. formájában. Ezt köteles ingyenesen rendelkezésére bocsátani. Amennyiben az érintett további másolatokat kíván igénybe venni, az adatkezelő az adminisztratív költségekért ésszerű mértékű díjat számíthat fel. Ha elektronikusan történik az adatigénylés, úgy az adatkezelő széles körben használt formátumban bocsáthatja rendelkezésre az információkat. Ügyelni kell mindeközben arra, hogy a másokra vonatkozó információkat hozzáférhetetlenné kell tenni. Ennek a jognak az újdonsága abból áll, hogy az érintettnek nem csak arra van joga, hogy tájékozódjon arról, hogy milyen adatokat kezelnek róla, hanem arra is, hogy elkérje a személyes adatot tartalmazó adathordozót és annak másolatát.
1. **Adatok helyesbítésének kérése:**
* Az érintett kérésére korrigálni kell indokolatlan késedelem nélkül az érintettre vonatkozó személyes adatokat.
1. **Törléshez való jog:**

Az érintett akkor jogosult arra, hogy töröltesse az adatokat indokolatlan késedelem nélkül, ha már a személyes adatokra nincs szükség abból a célból, amelyre eredetileg azokat gyűjtötték az érintett visszavonja adatkezelési hozzájárulását, így az adatkezelésnek nincs jogalapja az érintett adatkezelése ellen tiltakozik, és nincs más jogszerű ok az adatkezelés elvégzésére a személyes adatok jogellenesen lettek kezelve.

1. **Az adatkezelés korlátozásához való jog**
* Az érintett akkor kérheti, hogy adatkezelését korlátozzák, ha vitatja személyes adatainak pontosságát jogellenes az adatkezelés, az érintett viszont ellenzi az adatainak törlését többé már nincs szüksége az adatkezelőnek az adatokra, azonban az érintett a jogi igényeinek érvényesítéséhez megőrizné.
1. **Tiltakozáshoz való jog**
- Az adatkezelők tevékenységének transzparensnek kell lennie az érintettek számára, akik az adataik felett közvetlenebb módon rendelkezhetnek, így hozzáférhetnek, korrigáltathatnak vagy törölhetnek.
2. **Adathordozhatósághoz való jog**
* Az érintettnek joga van arra, hogy az adatkezelő által kibocsátott személyes adatait széles körben használt formátumban megkapja, amennyiben a személyes adatainak kezelése szerződésen vagy hozzájáruláson alapul, illetve az adatkezelés automatizált.
1. **Automatizált adatkezelés**

Az érintettnek joga van arra, hogy őrá ne terjedjen ki a kizárólag automatizált adatkezeléssel történő döntés hatálya.

* Adatai törlését bárki az adatkezelőhöz címzett nyilatkozattal kérheti szóban, írásban, postai címen, e-mail címen, weboldalon
* 2018. május 25. napjától nem szükséges már az adatvédelmi nyilvántartásba történő bejelentkezés. Előtte – vagyis jelenleg is – még adatkezelésenként külön adatvédelmi nyilvántartásba-vétel szükséges.
* A szabályok szerint egy személy fotója, képmása személyes adatnak minősül (biometrikus adat). Ha tehát emberek fotózása történik, legyen az modell, riport, rendezvény vagy esküvő, akkor emberek képmásainak őrzése megvalósul, legyen az egy telefon memóriája, egy profi fényképezőgép memóriája, vagy bármilyen háttértár, ahova azok lementésre kerülnek. Ez alapján, ha pl. céges rendvezvényt fotóz, akkor csak úgy tárolhatóak a képek a számítógépen, ha ehhez ő maga kifejezetten hozzájárult.
* Adatvédelmi tisztviselő:
- Az adatfeldolgozó és az adatkezelő köteles adatvédelmi tisztviselőt kijelölni, amennyiben a legfőbb feladatuk olyan műveletek, mint az érintettek rendszeres és nagymértékű megfigyelése vagy pedig különleges személyes adatok nagymértékű kezelése. Ezen kötelezettségen kívül bármely vállalkozás kinevezhet adatvédelmi tisztviselőt. Ha a vállalatnak nincs ilyen jogszabályi kötelezettsége és úgy dönt, hogy nem szükséges adatvédelmi tisztviselőt kinevezni, mert nem jár üzleti előnnyel, vagy túl nagy pénzügyi terhet jelentene, akkor ezt dokumentálnia kell a releváns tényekkel, indokokkal és szempontokkal, hogy a hatóságnak ez be tudja mutatni. Így teljesül ugyanis az elszámoltathatóság elve.

- A GDPR szigorúan védi az adatvédelmi tisztviselő feladatkörét és személyét, aki teljes szakmai függetlenséget élvez, utasításokat pedig senkitől sem fogadhat el feladatai ellátására vonatkozóan. Az adatfeldolgozó vagy az adatkezelő az adatvédelmi tisztviselőt feladataira hivatkozva nem sújthatja szankcióval és nem bocsáthatja el. Az adatvédelmi tisztviselő közvetlenül a legfelső vezetésnek tartozik felelősséggel. Vállalkozási szerződés alapján is elláthatók feladatai kiszervezett tevékenységként és munkavállalóként.

* **Feladatai**:
1. Adatvédelmi kérdésekben tájékoztat és tanácsot ad az adatfeldolgozó vagy az adatkezelő, illetve az ezeket a munkálatokat végző alkalmazottak részére.
2. Ellenőrzi, hogy a munkálatok megfelelnek-e az adatvédelmi szabályzatnak, ideértve az adatfeldolgozás és adatkezelés teljes szakaszát, úgy, mint a feladatkörök kijelölését, a munkavállalók képzését, és az ezekhez a feladatkörökhöz tartozó auditokat.
3. Az adatvédelmi hatásvizsgálat elvégzését nyomon követi, és ezzel kapcsolatban szakmai tanácsot ad.
4. A felügyeleti hatósággal együttműködik.
5. Kapcsolattartó a felügyeleti hatóság felé, illetve konzultációt folytat a hatósággal.
6. Akkor köteles az adatvédelmi tisztviselő **hatásvizsgálatot** készíteni, amennyiben igen magas kockázattal jár az érintettek jogaira és szabadságára nézve az adatkezelés. Ilyen eset lehet pl. a különleges adatok igen nagy számban való kezelése.