Gyakorlati javaslatok sportszervezeteknek a GDPR rendeletben foglaltaknak megfelelő adatkezelésre vonatkozóan

Mi az a GDPR?
Az Európai Parlament és a Tanács a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről szóló – és 2018. május 25. napjától alkalmazandó – (EU) 2016/679 rendelete.

Milyen változást hoz?
Megváltozik a személyes adat fogalma, az új rendelet az eddigieket kibővíti, így szükséges meghatározni, hogy a szervezet milyen személyes adatokat kezel.

Kire vonatkozik?
Mindenkire, aki személyes adatot kezel.

Mi minősül személyes adatnak?
Azok az azonosításra alkalmatlanná tett, titkosított vagy álnevesített személyes adatok, amelyek felhasználhatóak egy személy újraazonosítására.
Példák személyes adatra

- *vezetéknév és utónév;*
- *lakcím;*
- *a vezetéknév.utónév@vállalkozás.com típusú e-mail-címek;!*
- *személyazonosító igazolvány száma;*
- IP-cím;

A sportszervezetekre vonatkozik a GDPR?
Miután mindegyikük kezel személyes adatokat, ezért igen.

Ki az adatkezelő, ki az adatfeldolgozó?

Az adatkezelés magában foglal szinte minden, a személyes adatokon végzett cselekményt, így pl. azok felvételét, gyűjtését, tárolását, különböző célokra történő felhasználását, továbbítását, módosítását. Az ezt végző személy az Adatkezelő.
Az, aki az adatkezelő megbízásából és nevében személyes adatokkal dolgozik, az Adatfeldolgozó. A fontos különbség az, hogy míg az adatkezelő *meghatározza* az adatkezelés célját is, azaz dönt az adatok sorsáról, addig az adatfeldolgozó csak *az adatkezelő utasításai alapján* végez – jellemzően technikai – műveleteket az adatokon (pl. webtárhely szolgáltatója).

Néhány hasznos tanács az elején:

- csak olyan adatok legyenek a sportszervezetek birtokában, amelyekre bizonyíthatóan szükség van;
- ezeket megfelelően kell tárolni és folyamatosan átnézni, hogy mire van még szükség, és mi az, amit meg kell semmisíteni;
- az aktualitásukat vesztett adatokat, bizalmas információkat tartalmazó iratokat szakszerűen és biztonságosan kell megsemmisíteni, ehhez a megfelelő eszközöket időben be kell szerezni;
- a magánszemélyeknek ezek után is joga lesz betekintést kérniük abba, hogy hol és hogyan tárolják a róluk szóló adatokat, hogyan mozgatják azokat, illetve kellő időben megsemmisítik-e azokat;
- egy sportszervezetnél csak az erre kijelölt személyek férhetnek hozzá az adatokhoz; külön rendelkezni kell arról, hogy harmadik személynek milyen adatokat lehet átadni;
- át kell nézni a szerződéseket, beleértve a munkaszerződéseket is, és meg kell vizsgálni, hogy azok megfelelnek-e az új előírásoknak, illetve azoknak megfelelő szerződésmintákat kell kidolgozni;
- a személyes adatokhoz hozzáférő beszállítókkal, alvállalkozókkal a rendeletben foglalt előírásoknak megfelelő szerződést kell kötni;
- az esetleges beszerzési folyamatokba be kell építeni elvárásként a rendeletnek való megfelelést, különösen az alapértelmezett adatvédelem (privacy by design) követelményének való megfelelést;
- bizonyos feltételek teljesülése esetén ki kell nevezni egy adatvédelmi felelőst.

Melyek a főbb feladatok?

Első lépésként a jelenleg kezelt adatvagyont kell felmérni. A sportszervezeteknek be kell azonosítania, hogy milyen személyes adatokat tárol és használ, és mindezt milyen jogalapon, milyen célból teszi. Jogalapot teremt jogszabály, jogos érdek, kivételes esetben hozzájárulás. Legegyszerűbb ezt egy excel táblában megtenni, mintát csatolunk.
Jogalap hiányában a személyes adatokat törölni kell. Az adattérképben fel kell tüntetni azt is, amikor egy érdeklődő, kérelmező küld egy e-mailt vagy betelefonál és felírjuk az adatait (mi lesz ezután az adattal, ki hova továbbítja, mi a végállomás, ki fogja kezelni, majd tárolni és megsemmisíteni). Vagy valaki közérdekű adatot igényel, bejelent, panaszkodik, bármit tesz, amihez adja nevét, telefonszámát, e-mail címét vagy más azonosító adatát. Az adattérkép elkészítésére nincs forma, csinálhatjuk Excel-táblában vagy akár papír alapon is. Egy a lényeg: teljes körű legyen

Gyakorlatban – elvben – a kockázatelemzésünk alapjai között található egy vagyonleltár az adatgazdák kijelölésével. Itt érdemes kezdeni a felkészülést. Fel kell mérni, hogy mely területek – mely adatgazdák esetén – szembesülünk személyes adattal. Például HR, könyvelés, marketing, pénzügy és utalások, egyéb területek.

<u>Második lépésként</u> a sportszervezetnek be kell azonosítania, hogy a jövőben az érintettek mely személyes adatait kezeli, illetve az adatkezelési folyamatok során ki lesz jogosult a személyes adatokhoz hozzáférni. Arról is döntést kell hoznia, hogy amennyiben történik adatkezelés, úgy a személyes adatokat meddig tárolja. Itt természetesen be kell azonosítania azokat a jogszabályokat, amelyek a sportszervezetet, érintettet meghatározott személyes adatok őrzésére kötelezik. Minden egyes adatkezelésre vonatkozóan át kell tekinteni, hogy jogszerű-e, van-e hozzá jogalap, célhoz kötött-e, érvényesülnek-e a garanciális jogok, tájékoztatások.
Meg kell határozni, hogy milyen adatkezelések nem folytathatók tovább, mert jogilag védhetetlenek. Pl. hivatali gépeken vagy hivatali e-mail címen keresztül privát tartalom (pl.: a gyerekem óvodai fotóját küldik az óvodából) is bekerüljön a hivatal informatikai rendszerébe?

<u>Harmadik lépés - adattisztítás</u>
Ha már teljes körűen látható, hogy milyen adatkezeléseket végez a cég és már tudjuk, hogy milyen adatkezeléseket nem lehetséges jogszerűen tovább folytatni, akkor szükséges az adattisztítást végrehajtani. Ez annyit jelent, hogy megszüntetem, törlöm, elhagyom a védhetetlen adatkezeléseket, adatbázisokat, feljegyzéseket, listákat. A gyakorlatban ez járhat selejtezési, iratmegsemmisítési, fájltörlési cselekményekkel.

<u>Negyedik lépés Belső eljárásrendek, iratminták, tájékoztatók kidolgozása, oktatások megszervezése</u>
Ha már teljesen nyilvánvaló és akár vezetői szinten is eldöntött vagy jóváhagyott, hogy mely adatkezelések, milyen adatkörrel és mennyi ideig maradhatnak meg, akkor arra a szervezeten belül egy átlátható, védhető és az adatvédelmet beépített szemléletként és funkcióként kezelő eljárásrendi szabályrendszert kell kidolgozni. Iratmintákat biztosítunk.

<u>Ötödik lépés- Szabályzatok elkészítése</u>
El kell készíteni az adott sportszervezet adatkezelési szabályzatát és mindazokat az iratmintákat, amelyek szükségesek ahhoz, hogy az adatkezelésed megfeleljen a GDPR-nak. Mintákat biztosítunk.
az egész uniós rendelet központi magva az elszámoltathatóság, azaz legyen egyértelműen világos az adatkezelő számára, hogy milyen adatot, miért, milyen felhatalmazás alapján, hol tárolva, mennyi ideig kezel. Lássa át a rendszert, tudja bizonyítani, hogy (szinte) mindent megtett a magánszemélyek privát szférájának védelme érdekében és legyen tudatában, hogy igen magas bírsággal, akár több tíz vagy százmillió forintos bírságteherrel jár el egyszerű ügyintézőként is,
az adatkezelést mint tevékenységet, az egyes feladatokat, műveleteket tudni kell besorolni a kockázati szintek szerint, tudatában kel lenni, hogy az egyes cselekmények, eljárások milyen kockázattal járnak a magánszemélyek adataira nézve,
az összes adatkezelési műveletet, tevékenységet, eljárásrendet úgy kell megszervezni és kidolgozni, hogy a beépített adatvédelem elve érvényesüljön, azaz egy hatósági ellenőrzéskor is tudjuk bizonyítani, hogy a fentiek során vagy bármilyen szoftver alkalmazása során is maximális tekintettel voltunk az adatvédelem szabályrendszerére,
az adatkezelési tevékenységet folyamatosan monitorozni, ellenőrizni, szükség esetén változtatni kell. Folyamatos képzést, oktatást kell az adatkezelést végzők részére biztosítani (dokumentáltan!), hogy tudjuk igazolni majd az adatvédelmi hatóságnak.

A GDPR az adatkezelő felelősségévé teszi, hogy bármikor képes legyen bizonyítani a rendelet adatvédelmi elveinek való megfelelést!

Szükség van adatvédelmi tisztviselőre egy sportszervezetnél?
Az attól függ, hogy a működés indokolja-e Adatvédelmi tisztviselő kijelölését. Az alábbi esetekben mindenképpen kötelező:
ha az adatkezelő vagy az adatfeldolgozó fő tevékenységei különleges személyes adatok nagy számban (a gyakorlat szerint ez min. 1000-1200 főt jelent) történő kezelését foglalják magukban;
ha az adatkezelést közhatalmi szervek vagy egyéb, közfeladatot ellátó szervek végzik-ez nem vonatkozik a sportszervezetekre;
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 szervezetek természetesen önkéntes alapon is jelölhetnek adatvédelmi tisztviselőt, akik nagyban segíthetik a GDPR alkalmazására való felkészülést. A szervezetek természetesen alkalmazhatnak külön külső szakértőket, akik tanácsadóként járnak el, ekkor azonban egyértelműen meg kell jelölni, hogy ők nem adatvédelmi tisztviselők.

Adatvédelmi incidens, bejelentési kötelezettség

Új előírás, hogy bejelentési kötelezettség keletkezik az adatkezelő oldalán ún. adatvédelmi incidensek, azaz személyes adatokkal kapcsolatos jogsértések esetén, az adatkezelő általi tudomásszerzést követően haladéktalanul, de legkésőbb 72 órán belül. Kivétel ez alól, ha a személyes adatok megsértése „valószínűsíthetően” (ezt persze nehéz konkretizálni) nem okoz nagy sérelmet az érintettek számára. A bejelentést ilyenkor a NAIH felé kell megtenni. Az incidenssel érintett személyeket csak akkor kell értesíteni, ha az adatsértés számukra valószínűsíthetően nagy kockázatot jelent, pl. banki kódok kiszivárgása esetén. Ha az adatfeldolgozó észlel jogsértést, ő is köteles ezt bejelenteni, mégpedig az adatkezelő felé.