Figyelem: GDPR 

dióhéjban az Általános Adatvédelmi Rendeletről

dr. Petőcz Judit

Bakonybél, 2018. február 25.

Magyar Szabadidősport Szövetség

2016/679/EU (General Data Protection Regulation,GDPR)

Eddig érvényben lévő irányelv: 95/46/EK irányelv → ELAVULT

- **Kihirdetés:** 2016. április 27. dátummal az Európai Unió Hivatalos Lapjában
- **Hatálybalépés:** 2016. május 25.
- **Alkalmazás:** 2018. május 25-től!
  - közvetlenül, kötelezően alkalmazandó minden szervezetnél, amely személyes adatot kezel
  - felülírja a nemzeti jogszabályokat (2011. évi CXII. tv.(Info tv.))
- **Alkalmazkodás:**
  - jogharmonizáció még nem előrehaladott
  - Info tv.: új tervezet 2018. októberében kerül benyújtásra a Parlamentnek

Miért szükséges a rendelet?

- **Alapvetése:** a természetes személyek személyes adatainak védelme alapvető jog

De: *„A személyes adatok Unión belüli* ***szabad áramlása nem korlátozható vagy tiltható meg*** *a természetes személyeknek a személyes adatok kezelése tekintetében történő védelmével összefüggő okokból.”*

- nagyobb tudatosság az adatkezelés területén (adatkezelők és természetes személyek részéről is)
- nagyobb biztonság
- magánszemélyek online szolgáltatásokba vetett bizalmának megerősítése
- online környezethez jobban illeszkedő jogszabály

Miért fontos a megfelelés?

- A rendelet az egész Európai Unió területén hatályos, **kötelezően alkalmazandó**
- **Minden szervezetre** kiterjed, amely személyes adatot kezel
- **Folyamatos** nyomon követést, adminisztrációt jelent
- A nem megfelelés **következménye**:
  - bírság (cég éves bevételének 4%-a, maximum 20 millió Euro)
  - per
- **Ellenőrzés:**
  - NAIH (Nemzeti Adatvédelmi és Információszabadság Hatóság)
  - EDPB (European Data Protection Board): nemzetek feletti szervezet, tanácsadó, javaslattevő szerep


ELVEK
GDPR
Érintett jogai
Adatkezelő kötelezettségei
HOGYAN feleljünk meg?

➢ „személyes adat”:

- azonosított vagy azonosítható természetes személyre („érintett”) vonatkozó bármely információ;
- azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható.

➢ „adatkezelés”:

- a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így
- a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés, továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés.

Személyes adatok kezelésének elvei - joghézagok kitöltésére

- **Jogszerűség, tisztességes eljárás és átláthatóság:** az érintett számára átlátható módon
- **Célhoz kötöttség:** gyűjtés és kezelés csak meghatározott, egyértelmű és jogszerű célból
- **Adattakarékosság:** megfelelőek és relevánsak és csak a szükségesre korlátozódjanak
- **Pontosság:** pontosság és naprakészség; pontatlan személyes adatokat haladéktalanul töröljék vagy helyesbítsék
- **Korlátozott tárolhatóság:** az érintettek azonosítását csak az adatkezelési célok eléréséhez szükséges ideig teszi lehetővé
- **Integritás és bizalmas jelleg:** adatkezelést 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 védelme
- **Elszámoltathatóság:** szuperalapelv - az **adatkezelő felelős** a fentieknek való megfelelésért, továbbá képesnek kell lennie e **megfelelés igazolására**

Az érintett jogai

➢ Átlátható tájékoztatás és kommunikáció:

- érthető, könnyen hozzáférhető formában,
- világosan és közérthetően megfogalmazva,
- írásban vagy más módon (elektronikus úton),
- szóban is, feltéve, hogy más módon igazolták az érintett személyazonosságát

➢ Tájékoztatás és a személyes adatokhoz való hozzáférés

- Különbség aszerint, hogy a személyes adatokat az érintettől vagy nem az érintettől gyűjtik.

➢ Az érintett hozzáférési joga

- Személyes adatainak kezelése folyamatban van-e?
- Hozzáférjen meghatározott információkhoz

➢ Helyesbítéshez való jog

- indokolatlan késedelem nélkül helyesbíteni az érintettre vonatkozó pontatlan személyes adatokat,
- érintett kérheti a hiányos személyes adatok kiegészítését

➢ Törléshez való jog („az elfeledtetéshez való jog”)

- érintett kérheti, hogy indokolatlan késedelem nélkül töröljék személyes adatait
- indokolatlan késedelem nélkül törölni kell

➢ Az adatkezelés korlátozásához való jog

- Példálódzó felsorolás

pl.: érintett vitatja az adatok pontosságát: adatok ellenőrzésének idejére korlátozni

Adatkezelő **értesítési kötelezettsége**: helyesbítésről, törlésről, korlátozásról minden címzettet tájékoztatni, akivel a személyes adatot közölték,

kivéve: ha lehetetlen vagy aránytalanul nagy erőfeszítést igényel!

➢ Adathordozhatósághoz való jog

➢ Tiltakozáshoz való jog

➢ Automatizált döntéshozatal egyedi ügyekben

Adatkezelő/adatfeldolgozó kötelezettségei

- **Az elszámoltathatóság kettős főszabálya:**

„Az adatkezelő
- az adatkezelés jellege, hatóköre, körülményei és céljai, valamint
- a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével
- ***megfelelő technikai és szervezési intézkedéseket*** hajt végre annak biztosítása és bizonyítása céljából,

hogy a személyes adatok kezelése e rendelettel összhangban történik.

Ezeket az intézkedéseket az adatkezelő ***felülvizsgálja*** és szükség esetén ***naprakésszé teszi***.”

- ***megfelelő belső adatvédelmi szabályok alkalmazása!***

Kulcsszó: **EGYEDIESÍTÉS !!**

HOGYAN feleljünk meg?

- Beépített és alapértelmezett adatvédelem
- Átalakuló adatkezelési jogalapok
- Adatkezelési tevékenységek nyilvántartása
- Adatvédelmi tisztviselő kijelölése
- Adatfeldolgozó kiválasztása
- Megfelelő adatbiztonsági intézkedések megtétele
- Adatvédelmi incidensek kezelése
- Adatvédelmi hatásvizsgálat

Beépített és alapértelmezett adatvédelem

Privacy by design/ Privacy by default

*„Az adatkezelő **megfelelő technikai és szervezési intézkedéseket** hajt végre annak biztosítására, hogy alapértelmezés szerint kizárólag olyan személyes adatok kezelésére kerüljön sor, amelyek az adott konkrét **adatkezelési cél szempontjából szükségesek** (adattakarékosság elve).”*

- IT biztonság: álnevesítés/pszeudonimizálás, anonimizálás, kriptográfiai műveletek beépítése
- adatbiztonsági kultúra és tudatosság kialakítása
- adatbiztonságért felelős személy kijelölése
- adatbiztonsági szabályzat elfogadása, oktatások
- adatok fizikai védelme (riasztók, kamerák, belépési szabályok, papírhulladék kezelése)

Átalakuló adatkezelési jogalapok

Mikor jogszerű az adatkezelés?

Kizárólag akkor és annyiban, amennyiben legalább az **alábbiak egyike** teljesül:

- az érintett **hozzájárulását adta**
- **szerződés teljesítéséhez** szükséges
- az adatkezelőre vonatkozó **jogi kötelezettség teljesítéséhez** szükséges
- az érintett vagy egy másik természetes személy **létfontosságú érdekeinek védelme miatt** szükséges;
- **közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány** gyakorlásának keretében végzett feladat végrehajtásához szükséges;
- **az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez** szükséges, **kivéve**, elsőbbséget élveznek az érintett egyéb érdekei vagy alapvető jogai és szabadságai, különösen, ha az érintett gyermek.

A hozzájárulás feltételei

Az érintett akaratának

- **önkéntes**,
- **konkrét**,
- **megfelelő tájékoztatáson** alapuló,
- **egyértelmű** kinyilvánítása,

amellyel az érintett **nyilatkozat** vagy a megerősítést félreérthetetlenül kifejező **cselekedet** útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez;

Az adatkezelőnek képesnek kell lennie annak **igazolására**, hogy az érintett személyes adatainak kezeléséhez hozzájárult.

Bármikor **visszavonható** – érintettet tájékoztatni!!!

HOGYAN? - pl. check boksz-szal, gombra klikkeléssel
ÁSZF elfogadásától elkülöníteni!

Gyermek hozzájárulása: csak ha 16. évét betöltötte

Adatkezelési tevékenységek nyilvántartása

„Minden adatkezelő és – ha van ilyen – az adatkezelő képviselője a felelősségébe tartozóan végzett adatkezelési tevékenységekről nyilvántartást vezet.”

- **Főszabály:** köteles írásban/elektronikus formában nyilvántartást vezetni, aki **250 főnél több munkavállalót** foglalkoztat

- **Kivételek:**
  - ha a végzett adatkezelés az érintettek jogaira és szabadságaira nézve valószínűsíthetően kockázattal jár;
  - ha az adatkezelés nem alkalmi jellegű; illetve
  - ha az adatkezelés kiterjed különleges személyes adatokra, vagy bűncselekményekre vonatkozó személyes adatokra.

FONTOS: a nyilvántartásunk az esetleges ellenőrzés alapja lesz!

Adatvédelmi tisztviselő kijelölése

Feladata annak ***előmozdítása és biztosítása***, hogy a szervezeten belül végzett adatkezelési tevékenységek megfelelnek a vonatkozó előírásoknak, illetve szervezeten kívülre irányuló kérdésekben ***elsődleges kontaktként*** jár el.

Mikor kötelező?

- közhatalmi szervek, közfeladatot ellátó szervek által végzett adatkezelés esetén
- ha az adatkezelő fő tevékenysége olyan adatkezelést foglal magában, amely az érintettek rendszeres és szisztematikus, nagymértékű megfigyelését (adatkezelést) teszi szükségessé (bankok, biztosítók, IT cégek, eü. szolgáltatók, stb.)
- ha nagy számban kezel az adatkezelő különleges adatot

Adatfeldolgozó kiválasztása

- **Ki?**
  - az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az **adatkezelő nevében** személyes adatokat kezel.

- **Alkalmazásának feltételei**
  - kötelező **írásbeli szerződésben megbízni** (ideértve az elektronikus utat is)
  - kizárólag olyan adatfeldolgozó vehető igénybe, aki megfelelő **garanciákat** nyújt a rendelet követelményeinek való megfelelését és az érintettek jogainak védelmét biztosító, **megfelelő technikai és szervezési intézkedések** végrehajtására

FONTOS: adatkezelő és adatfeldolgozó **egyetemleges kártérítési felelőssége! = közvetlenül felelősek és perelhetők**

Megfelelő adatbiztonsági intézkedések megtétele

*„megfelelő **technikai és szervezési intézkedéseket** [végrehajtani] annak érdekében, hogy a **kockázat mértékének megfelelő szintű** adatbiztonságot garantálja”*

- **Mit jelent?**
  - személyes adatok **álnevesítését, titkosítását**;
  - adatkezelésre használt rendszerek és szolgáltatások folyamatos **bizalmas jellegének** biztosítását, integritását,..;
  - **incidens esetén** a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását kellő időben **vissza lehet állítani**;
  - az adatkezelés biztonságának garantálására hozott technikai és szervezési **intézkedések hatékonyságának** rendszeres **tesztelésére**, **felmérésére** és **értékelésére** szolgáló **eljárást**.

Adatkezelő és adatfeldolgozó együtt is biztosíthatja, de **egyetemlegesen felelnek**!

Adatvédelmi incidensek kezelése

- Az adatkezelő **72 órán belül köteles bejelenteni** a felügyeleti hatóságnak (NAIH), **kivéve,**
  ha valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve.

- **Bejelentés kötelező tartalma:**
  - Incidens jellege – érintettek kategóriái és száma, érintett adatok kategóriái és száma
  - Adatvédelmi tisztviselő/kapcsolattartó személy neve és elérhetősége
  - Valószínűsíthető következmények ismertetése
  - Orvoslásra tett/tervezett intézkedések leírása

- Adatkezelő köteles **incidens-nyilvántartást** vezetni (a fenti adatokkal)

- Az **érintettek tájékoztatása kötelező**: ha az incidens **magas kockázattal** jár
  - A tájékoztatás tartalma megegyezik a bejelentés tartalmával
  - **Kivételek!** (pl. aránytalan erőfeszítés)

Adatvédelmi hatásvizsgálat

*„olyan eljárás, amelynek során az adatkezelő a tervezett adatkezelési **műveleteket áttekinti**, **megvizsgálja** az adatkezelés érintettekre gyakorolt esetleges **hatását**, **felméri** annak **kockázatait**, a kockázatok kezelésének módját – és mindezt megfelelően **dokumentálja**”*

- **Új jogintézmény**, célja az önkéntes megfelelés ösztönzése.
- **Nem kell nyilvánosságra hozni**, kivonat készítése érdemes lehet.
- **Mikor kötelező?**
  - Adatkezelés valószínűsíthetően magas kockázata (ezekről lesz EU jegyzék)
  - Automatizált döntéshozatalon alapuló adatkezelések (profilalkotás)
  - Különleges személyes adatok, ill. büntetőjogi felelősségre vonatkozó személyes adatok
  - Nyilvános helyek nagymértékű, módszeres megfigyelése

Záró gondolatok

- Fő az **egyediesítés**: nincsenek általános alkalmazható megoldások, szervezetenként eltérően kell kialakítani az adatkezelési gyakorlatot.

- A joggyakorlat kialakulásáig a **„követendő” út**:

  - pozitív vállalati hozzáállás: önkéntes és előzetes megfelelés (privacy by design),
  - szervezeten belüli szoros együttműködés,
  - tudatosság növelése, adatbiztonsági kultúra meghonosítása
  - megfelelő szerződések megkötése,
  - belső adatvédelmi felelős kijelölése,
  - folyamatos önellenőrzés

- És amiről **nem beszéltünk**:
  - munkáltatókra vonatkozó szigorúbb szabályok
  - Online marketing és honlapkezelés

Köszönöm a figyelmet!

petocz.judit@masport.hu

Magyar Szabadidősport Szövetség