**UNIÓS ADATVÉDELMI RENDELET – 2018. MÁJUS 25.**

**GDPR**

A jelen cikkben tájékoztatni szeretnénk Tagtársainkat a sajtóban hetek óta egyre fokozódóan emlegetett **GDPR (azaz General Data Protection Regulation** – az Európai Parlament és Tanács 2016/679. számú rendelete) szabályokkal kapcsolatban, a teljesség igénye nélkül kiemelve egy-két olyan fontos újdonságot, amely a pszichológusi munkát jelentősen érinti, befolyásoja 2018. május 25-t követően.

**Jelenleg** elsősorban

* az információs önrendelkezési jogról szóló 2011. évi CXII. törvény (Infotv.)
* az egészségügyről szóló 1997. évi CLIV. törvény (Eütv) és
* az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény (Eüak)

szabályozza, hogy hogyan kell kezelni az egészségügyi tevékenység keretében megszerzett személyes adatokat.

**A jelenlegi szabályok is elég szigorúak, azok teljesítése tekintetében is sok hiányosságot lehet tapasztalni** az egészségügyi és a nem egészségügyi pszichológiai szolgáltatások területén egyaránt. **2018. május 25-től a GDPR szabályai lesznek elsősorban alkalmazandók**, melyeket kiegészítenek majd a nemzeti jogszabályok. Emiatt a fenti listában szereplő törvényeket szükségképpen módosítani kell majd, illetve újabb jogalkotás is várható, hogy segítse a GDPR hazai alkalmazását.

**A GDPR szabályainak a megismerése elengedhetetlenül szükséges az egészségügyi adatokat, vagy a nem egészségügyi területen tevékenykedő, de ugyanúgy személyes adatokat kezelő pszichológus kollégák által.** Ehhez **javasoljuk, hogy forduljanak szakemberhez** a kedves Tagtársak, mert a szakmai sajtó olvasása bizonyosan nem biztosít elég információt, személyre szabott szakmai tanácsot a felkészüléshez.

A felkészülés annál is inkább fontos, mert a GDPR hatálybalépésével bekövetkező egyik legnagyobb változás az **a legmagasabb kiszabható bírságösszegek extrém emelkedése** (az Infotv-ben rögzített 20.000.000 forint helyett 20.000.000 euro, nem forint!). A bírságolás gyakorlatát ugyan a NAIH fogja majd kialakítani, de a GDPR bevezetését segítő uniós 29-es Munkacsoport ajánlása szerint a bírságolásnak harmonizált gyakorlatát kell kialakítani az egyes tagállamokban, hogy ne alakulhasson ki a "bírságturizmus".

Ezen kívül csak példálózó jelleggel, a felkészüléshez való kedvcsinálóként fel szeretnénk hívni a figyelmet a többségében a jelenlegi szabályozás alapján is érvényes, azonban a GDPR által hangsúlyosabbá váló, **az adatkezelés során betartandó egy-két fontos rendelkezésre**.

* **Minden személyes adat**, amely akár némi erőfeszítés árán, de összekapcsolható valamely természetes személlyel: így pl. személyes adat lehet egy IP cím is, ha a hírközlési szolgáltatótól megszerezhető információ alapján összekapcsolható az előfizetővel. **A kutatások során névvel ellátott beleegyező nyilatkozat kódszáma alapján előbb-utóbb összeköthető a kérdőívekel. A betegek minden adata kiemelten személyes adat!**
* Szintén személyes adatkezelés történik, ha a kódokkal álnevesített személyek esetében nincs megfelelően biztosítva, hogy a személyt és a kódot ne lehessen összekapcsolni.
* Személyes adatot csak a GDPR rendeletben szereplő **jogalapok** alapján lehet kezelni, azaz minden egyes adatkezelésnél meg kell előzetesen állapítani, hogy a GDPR-ban rögzített valamely jogalapra tekintettel az jogszerű-e. **Pl. a pszichológus csak akkor érhet el kiemelten személyes adatot (bármit, ami egészségügyi adatnak minősül), ha ehhez képzettsége, működési engedélye vagy egyéb engedélyezett kutatási nyomós oka van.**
* Az **érintettnek széleskörű jogai** vannak, amelyeket késedelem nélkül teljesítenie kell az adatkezelőnek, ha az érintett igényli. Ilyen érintetti jog például, hogy
	+ minden esetben a GDPR szerinti tájékoztatást megkapja, mielőtt a személyes adatait kezeli az adatkezelő,
	+ visszavonhassa a hozzájárulást az adatkezeléshez, ez esetben pedig meg kell azt szüntetni, ha az érintett hozzájárulása volt a jogalapja az adatkezelésnek,
	+ bármikor tájékoztatást kapjon, hogy mely adatát és hogyan kezeli az adatkezelő, ez adott esetben azt is jelentheti, hogy betekintést kérhet a kezeléséről készült dokumentációba,
	+ kérheti az adatkezelés korlátozását.
* Különböző **nyilvántartásokat** kell vezetnie az adatkezelőnek, például
	+ a kezelt adatokról,
	+ a harmadik személy részére való adattovábbításokról,
	+ az érintettek által benyújtott kérelmekről (tájékoztatás, hozzáférés, korlátozás, stb.)
	+ az esetleges adatvédelmi incidensekről (amikor sérülnek az érintettnek a személyes adatokhoz fűződő jogai valamilyen váratlan esemény miatt, pl. adatvesztés történik)
	+ azok megoldásáról, a Hatóságnak tett bejelentésekről.
* Célszerű **belső szabályzatot** készíteni a szolgáltató működése keretében végzett adatkezelés szabályairól. Ez zömében hiányzik ma a pszichológiai tanácsadásokon, kutató intézetekben, egyetemeken és a rendelőkben. Május 25-ig ezt el kell készíteni.
* Az **adatkezelés biztonságát** folyamatosan tesztelni, ellenőrizni kell, erre vonatkozó belső eljárást kell kialakítania minden adatkezelőnek. (Ebben **az adatvédelmi tisztviselő ad informatikai, jogi tanácsot)**
* Szigorú adatbiztonsági feltételeknek kell megfelelnie minden adatkezelőnek:
	+ biztosítania kell, hogy az általa kezelt adatokhoz illetéktelenek ne férjenek hozzá,
	+ az adatok ne módosuljanak,
	+ ne semmisüljenek meg, és
	+ ne kerüljenek nyilvánosságra.
	+ Megadott ideig őrizve legyenek

Ezeket biztosítania kell egyfelől az adatok tárolása során (pl. a saját számítógépe, szervere, iratszerkénye ne legyen feltörhető), másfelől az adatok továbbítása esetén is (biztonságos csatornán továbbítsa, garantálja, hogy csak a címzett kezébe jut és nem máshoz, stb.).

* Az egészségügyi adatokat kezelő szervezeteknek, személyeknek **adatvédelmi tisztviselőt** kell kijelölnie. **Akkor is, ha egyszemélyes magánpraxisban kezel egészségügyi adatokat (!!!).** A tisztviselő ellenőrzi, hogy az adatkezelő a GDPR-nak megfelelően működik-e, e tekintetben tanácsot ad, kapcsolatot tart a felügyeleti hatósággal.

A GDPR lehetőséget nyújt a szakmai szervezetek részére, hogy **magatartási kódex** kialakításával segítsék a szakmatársak megfelelő adatkezelését. Amennyiben a felügyeleti hatóság jóváhagyja a magatartási kódexet, úgy annak betartásával az adatkezelők igazolni tudják, hogy a GDPR-nak megfelelően működnek. Az MPÉE szándéka szerint létre kíván hozni és az időközben remélhetőleg kijelölésre kerülő felügyeleti hatósághoz jóváhagyásra be kívánja nyújtani a pszichológiai tevékenység adatkezelésének magatartási kódexét a tisztelt Tagtársak adatkezelési tevékenységének a megkönnyítésére.