Tisztelt Munkatársak!

Az Európai Unió új általános adatvédelmi rendelete („General Data Protection Regulation” - **GDPR**) 2018. május 25-étől Magyarországon is alkalmazandó.

Az új EU-s szabályozással szigorodnak a személyes, azon belül az egészségügyi adatok kezelésére vonatkozó szabályok**. Az adatvédelmi hatóság a GDPR rendelkezéseinek betartását ellenőrizheti, a szabályok megsértése esetén bírságot szabhat ki, melynek összege a jogsértés súlyától függően akár 20 millió EUR is lehet.**

A Pécsi Tudományegyetem Klinikai Központ eddig is nagy hangsúlyt fektetett a mindenkor hatályos adatvédelmi jogszabályok és szabályzatok betartására, az egészségügyi ellátás során keletkezett adatok kezelésére és őrzésére. Ezen célok betartását továbbra is fontosnak tartjuk, ezért egy rövid tájékoztatást adunk a GDPR legfontosabb rendelkezéseiről.

Személyes adat az azonosított vagy azonosítható természetes személyre vonatkozó bármely adat.
Azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító - pl. név, azonosító 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.
A GDPR kifejezetten személyes adatként nevesíti a helymeghatározó adatokat és az online azonosítókat, például IP-címek és cookie-azonosítók, valamint egyéb azonosítók, például rádiófrekvenciás azonosító címkék.

Különleges adatnak minősül a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a természetes személyek egyedi azonosítását célzó genetikai és biometrikus adatok, az **egészségügyi adatok** és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok. Ezek kezelése **alapvetően tilos**.

A GDPR meghatározza, hogy mely esetekben **lehet** mégis ezen **adatokat kezelni**, többek között, ha az érintett kifejezett hozzájárulását adta, uniós vagy tagállami jog lehetővé teszi (pl. bírósági eljárások, közérdek, **egészségügyi** vagy szociális **ellátás** vagy kezelés nyújtása, népegészségügy…).

A **hozzájárulás** az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló és 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.

Ha az adatkezelő a személyes adatokon a gyűjtésük céljától eltérő célból további adatkezelést kíván végezni (pl. kutatás), **a további adatkezelést megelőzően tájékoztatnia kell** az érintettet erről **az eltérő célról** és minden releváns kiegészítő információról.

Az érintett jogosult a hozzájárulását bármikor visszavonni.

A GDPR rendelkezéseit **nem kell alkalmazni** olyan információkra, amelyek anonimizáltak, amelynek következtében az érintett nem vagy többé nem azonosítható. Az álnevesített személyes adatokat, amelyeket további információ felhasználásával valamely természetes személlyel kapcsolatba lehet hozni, azonosítható természetes személyre vonatkozó adatnak kell tekinteni.

A személyes adatkezelésben **érintett jogosult** arra, hogy az adatkezelőtől **tájékoztatást** kapjon a személyes adatainak kezeléséről és jogosult arra, hogy **hozzáférést** kapjon az adatokhoz, továbbá információt kapjon az adatkezelés **céljairól, jogalapjáról**, kategóriáiról, az adatok tárolásáról, ennek időtartamáról.
Kérelmezheti az adatkezelőtől adatai helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az adatok kezelése ellen. Tájékoztatni kell az adatkezeléssel kapcsolatos **panasz benyújtásának lehetőségéről.**

A személyes adatok, ezen belül az egészségügyi adatok kezelése során az alábbi **alapelvek** figyelembe vételével kell eljárni:

Jogszerűség, tisztességes eljárás és átláthatóság: a személyes adatokat jogszerűen, tisztességesen, és az érintett számára átlátható módon kell kezelni.

Célhoz kötöttség: a személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történjen, és azokat ne kezeljék ezekkel a célokkal össze nem egyeztethető módon.

Adattakarékosság: a személyes adatok az adatkezelés céljai szempontjából megfelelőek és relevánsak kell, hogy legyenek, és a szükségesre kell korlátozódniuk.

Pontosság: a személyes adatoknak pontosnak és szükség esetén naprakésznek kell lenniük. Minden észszerű intézkedést meg kell tenni annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul töröljék vagy helyesbítsék.

Korlátozott tárolhatóság: a személyes adatok tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak az adatkezelés céljainak eléréséhez szükséges ideig teszi lehetővé.

Integritás és bizalmas jelleg: 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.

Elszámoltathatóság: a gyakorlatban ez azt jelenti, hogy az adatkezelő felelős a fenti hat alapelvnek való megfelelésért, továbbá képesnek kell lennie e megfelelés igazolására.

Az adatkezelő és az adatfeldolgozó köteles biztosítani a megfelelő **adatbiztonság**ot a tudomány és technológia állása, a megvalósítás költségei, a változó valószínűségű és súlyosságú kockázat figyelembevételével.

Az adatbiztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, módosítását, jogosulatlan nyilvánosságra hozatalát vagy azokhoz való jogosulatlan hozzáférést eredményezi, **adatvédelmi incidens**nek minősül. Az adatkezelő az adatvédelmi incidensekről **nyilvántartást vezet** és indokolatlan késedelem nélkül, ha lehetséges, legkésőbb a tudomásra jutástól számított **72 órán** belül **be kell jelentenie** az adatvédelmi hatóságnak.

Az adatkezeléssel kapcsolatos jogszabályok és szabályzatok teljesítése és az érintettek jogainak érvényesítése érdekében az adatkezelő és az adatfeldolgozó a belső adatvédelmi felelősök helyett **adatvédelmi tisztviselő**ket nevezhetnek ki.

A GDPR szerint adatvédelmi tisztviselő kijelölése sok esetben kötelező, például különleges (egészségügyi) adatok kezelése esetén, így egészségügyi intézményekben is.

Az adatkezelőnek vagy az adatfeldolgozónak közzé kell tennie az adatvédelmi tisztviselő nevét és elérhetőségét, és azokat az adatvédelmi hatósággal közölnie kell.

A Pécsi Tudományegyetemen adatvédelmi tisztviselő, illetve a PTE Klinikai Központban egészségügyi adatvédelmi tisztviselő kerül kinevezésre.

A Pécsi Tudományegyetem új, a GDPR rendelkezéseinek megfelelő, adatvédelmi szabályzatát 2018.05.23-án elfogadta a Szenátus, a PTE új egészségügyi adatvédelmi szabályzatát a Szenátus júniusi ülésén tárgyalja.

A GDPR minden EU-s tagállamban **közvetlenül alkalmazandó**, így nem kell külön tagállami jogszabály formájában átvenni. Az érintett adatkezelők, adatfeldolgozók és természetes személyek közvetlenül hivatkozhatnak a GDPR rendelkezéseire. Ennek ellenére várhatóan az az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény és az egészségügyi és hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény is változni fog.

Pécs, 2018. május 25.

PTE Klinikai Központ