Adatfeldolgozási megállapodás

Melléklet

A Felek jelen adatfeldolgozási megállapodással (a továbbiakban: **Megállapodás**) kiegészítik a közöttük **..... napján klinikai kutatás** elvégzésre létrejött megállapodásukat. A megállapodás értelmében a Megbízott, mint Adatfeldolgozó, a megbízó mint Adatkezelő nevében személyes adatokat dolgoz fel. A jelen Megállapodás meghatározza azon személyes adatok Adatfeldolgozó általi feldolgozásának és azokhoz történő hozzáférésének feltételeit, amelyekért az Adatkezelő felelős.
Felek a jelen szerződésük elválaszthatatlan mellékletenként megállapodnak az adatfeldolgozásra vonatkozó kérdésekben:

1. Irányadó/alkalmazandó rendelkezések („Adatvédelmi jogszabályok"), alkalmazandó jogszabályok:

Bármilyen jog, törvény, nyilatkozat, rendelet, utasítás, kormányrendelet, szabályozás, szabály vagy egyéb kötelező korlátozás szabályozás (a módosításainak, egységes szerkezetbe foglalásnak, újbóli hatálybaléptetésnek megfelelően), amely az egyének védelmére vonatkozik a személyes adatok kezelése tekintetében, különösen a 2016/679 sz. EU Rendelet a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről (az Általános Adatvédelmi Rendelet – GDPR), valamint bármiféle magatartási kódex vagy iránymutatás, amelyet a megfelelő felügyeleti hatóság időről időre kibocsát.

2. Fogalmak

Felek rögzítik, hogy megállapodásukban a fogalmak értelmezésekor, többek között, de nem kizárólagosan „személyes adat"; „adatkezelés"; „álnevesítés"; „anonimizálás"; „nyilvántartási rendszer"; „adatkezelő", „adatfeldolgozó", „címzett", „harmadik fél", „az érintett hozzájárulása", „adatvédelmi incidens", „bio-metrikus adat", „egészségügyi adat" a GDPR rendelkezéseit tartják irányadónak.

3. Felek adatkezelési tevékenységei, az adatkezelés tárgya, célja

3.1. **A FELEK KÖZÖTTI MEGÁLLAPODÁS CÉLJA**, a szerződésben meghatározott **klinikai kutatás** elvégzéséhez érdekében az adatkezelő (Megbízó) által adatok gyűjtése, az adatfeldolgozó (Megbízott) által ezen adatok gyűjtéséhez és adatok gyűjtése és adatfeldolgozása szolgáltatása .

3.2. Az adatok gyűjtésének és feldolgozásának célját és eszközeit a Megbízó határozza meg az alábbiak szerint:

3.3. **A MEGBÍZÓ UTASÍTÁSA**: A Megbízott személyes adatokat kizárólag a Megbízó dokumentált utasításainak megfelelően dolgoz fel. A Megbízó kizárólag írásban adhat további vagy eltérő utasítást, amely csak akkor kötelező, ha a Megbízott írásban visszaigazolta azt. A Megbízott köteles értesíteni a Megbízót arról, ha véleménye szerint valamely utasítás ellentétes a GDPR-rel vagy a Megbízottra, mint adatfeldolgozóra vonatkozó adatvédelmi rendelkezésekkel. A Megbízott nem köteles átfogó jogi felülvizsgálatot végezni vagy jogszabály által tiltott utasításokat végrehajtani. A Megbízó viseli a Megbízott oldalán a további vagy eltérő utasítások miatt felmerülő összes többletköltséget, kivéve, ha az utasításra a Megbízottra vonatkozó jogszabályi előírások betartása végett van szükség.

4. Személyes adatok köre, az érintettek kategóriái

4.1. A Felek rögzítik, hogy csak olyan személyes adatot kezelnek, melyek az adatkezelés céljai szempontjából megfelelőek és relevánsak és a szükségesre korlátozódnak. Az adatfeldolgozásba vont személyes adatok típusai ténylegesen valamennyi érintett személyes azonosító adatai, a kapcsolattartók kapcsolattartási adatai, a betegek egészségügyi és genetikai adatai.

4.2. A Megbízott csak és kizárólag olyan személyes adatot adhat át, melynek kezelésre a Megbízó utasította és amely a cél eléréséhez szükséges. **A Megbízott nem jogosult a vizsgálati alanyok olyan személyes adatai továbbítására, melyet a Megbízott szolgáltatói feladatának ellátása során kezel. A Megbízott a beteg adatokat álnevesítve adja át a Megbízó részére.**

4.3 **AZ ADATKEZELÉS JOGLAPJA** minden adat esetében az érintett betegnek a GDPR 9. cikk (2) bekezdésének a) pontja szerinti, a többi érintett esetén pedig a GDPR 6 cikkel (1) bek a) pontja szerinti hozzájárulása.

4.4. A Megbízó tudomásul veszi, hogy a Megbízott nem jogosult tájékoztatni a vizsgálatvezető múltbeli, továbbá a vizsgálat elvégzésére irányuló megállapodás hatályának megszűnését követő olyan tényleges vagy tervezett ideiglenes vagy végleges eltiltásról, felfüggesztésről, kizárásról, elítélésről, korlátozásról, illetve szankcióról vagy vizsgálatról, mely a Vizsgálatvezető jogi alkalmasságát, illetve vizsgálat elvégzésére irányuló megállapodásban rögzített vizsgálat elvégzését nem érinti.

5. Tájékozott beleegyezésen alapuló, önkéntes hozzájárulás

5.1. A GDPR 13-14. cikkek szerinti részletes tájékoztatás megadása/elkészítése az önálló adatkezelőként eljáró felet terheli. Az adatkezelő által elkészített tájékoztatót az érintett részére az adatfeldolgozó adja át és szerzi be a hozzájáruló nyilatkozatát az adatkezelő részére való átadására. Az adatfeldolgozó haladéktalanul tájékoztató az adatkezelőt, ha úgy véli, hogy annak ezen utasítása sérti a GDPR rendeletet és a tájékoztató nem felel meg a GDPR 13. illetve 14. cikkében előírtaknak. Az adatfeldolgozó minden erőfeszítést megtesz annak érdekében, hogy az önkéntes, kifejezett, tájékoztatáson alapuló és egyértelmű, célonként megadott hozzájárulási nyilatkozatot az érintett megtegye; azon érintettek adata nem kezelhető, akik az adatkezeléshez a hozzájárulásukat nem adták meg, vagy visszavonták.

5.2. Felek megállapodnak, hogy **az érintettek adatait a jelen szerződésben meghatározott céltól eltérő célra nem kezelik, ilyen adatkezelésre csak** érintett ismételt - a cél és jogalap megjelölést tartalmazó a GDPR 13. és 14. cikkének megfelelő tájékoztatása után kizárólag az érintett ismételt önkéntes, kifejezett, tájékoztatáson alapuló és egyértelmű, célonként megadott hozzájárulása alapján kerülhet sor.

6. A személyes adatok megőrzésének időtartama

Felek rögzítik, hogy a személyes adatokat csak és kizárólag a kezelésükre irányadó jogszabályokban meghatározott időpontig, illetve időtartamig őrzik meg. Alkalmazandó jogszabály rendelkezésének hiányában a személyes adatok megőrzésének időpontjára irányadó, hogy addig kerül megőrzésre, amíg kezelésére a cél elérése érdekében szükség, illetve valamely fél jogai, vagy kötelezettségei érvényesítésére jogszabályban rögzített elévülési idő áll fenn. A Felek rögzítik, hogy bizonytalan időtartamú, vagy határidejű jövőbeni cél elérése érdekében csak és kizárólag az érintett önkéntes,

kifejezett, tájékoztatáson alapuló és egyértelmű, célonként megadott hozzájárulása alapján kerülhet sor.

7. Személyes adatok Európai Gazdasági Térségen kívüli továbbítása

Személyes adat harmadik országba vagy nemzetközi szervezet részére történő továbbítására akkor kerülhet sor, ha az Európai Unió Bizottsága (a továbbiakban: Bizottság) megállapította, hogy a harmadik ország, a harmadik ország valamely területe, vagy egy vagy több meghatározott ágazata, vagy a nemzetközi szervezet a GDPR-ban előírt megfelelő védelmi szintet biztosít. A Bizottság határozatának hiányában ilyen országba, illetve szervezethez történő adattovábbítás megfelelő – GDPR 46. cikke szerinti – garanciákkal, illetve GDPR 49. cikk szerinti eltérésekkel történhet. Az adattovábbítást megelőzően a feleknek nyilatkoznia kell, hogy az adattovábbításhoz rendelkeznek a jelen pontban meghatározott megfelelő határozattal, garanciával, illetve jogalappal. A Megbízó ez esetben köteles a GDPR 44. és azt követő cikkeiben meghatározott adattovábbítási mechanizmusokat alkalmazni. A Megbízó köteles különösen kielégítő garanciákat nyújtani arra vonatkozóan, hogy meghozta a megfelelő technikai és szervezési intézkedéseket, amelyek biztosítják, hogy az adatkezelés megfeleljen a GDPR előírásainak, biztosítja az érintettek jogainak védelmét, nyilvántartja az adattovábbításokat és dokumentálja a megfelelő garanciákat. A Megbízó az Európai Bizottság 2010/87/EU határozata szerinti általános szerződéses feltételek vagy a GDPR 46. cikk szerinti általános adatvédelmi kikötések („általános adatvédelmi kikötések”) útján biztosíthatja ezeket a kielégítő garanciákat.

8. Alkalmazandó jogszabályoknak történő megfelelés

A Felek vállalják, hogy a vizsgálat elvégzésére irányuló megállapodásban rögzített vizsgálatot az alkalmazandó jogszabályok betartásával végzik el. A Felek mindegyike köteles létrehozni és fenntartani az Alkalmazandó jogszabályok által a személyes adatok feldolgozásához előírt nyilvántartásokat. A Felek együttműködnek és segítik egymást az olyan adatvédelmi hatásvizsgálatok és/vagy felügyeleti hatóságokkal való konzultációk kapcsán, amelyekre a vizsgálat elvégzésére irányuló megállapodás hatálya alatt történő adatkezelés vonatkozásában esetleg szükség van.

9. Adatbiztonság

A vizsgálat elvégzésére irányuló megállapodás időtartama alatt a Felek mindegyike - a GDPR 28. cikkének (3) bek c) pontjának megfelelően - köteles olyan adatbiztonsági intézkedést megtenni, amely biztosítja, hogy a személyes adatok kizárólag a vizsgálat elvégzésére irányuló megállapodással összhangban kerüljenek kezelésre. A Felek mindegyike köteles megfelelő adminisztratív, technikai és fizikai biztonsági intézkedéseket bevezetni a személyes adatok védelme érdekében. A Felek megteszik mindazon a technikai és szervezési intézkedéseket, figyelembe véve a tudomány és technológia állását, az adatfeldolgozás végrehajtási költségeit, jellegét, terjedelmét, összefüggéseit és céljait, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázatokat, különös tekintettel a személyes adatok kezelése jelentette olyan kockázatokra, mint például a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítése, elvesztése, megváltoztatása, jogosulatlan közlése vagy az azokhoz való jogosulatlan hozzáférés.

9.1. A Felek az adatbiztonság érdekében az alábbi technikai és szervezési intézkedéseket teszik:

9.1.1. Személyes adatok álnevesítése és titkosítás: A Megbízott a személyes adatokat oly módon különíti el a kezelt adatoktól, hogy a kezelt adatokat a külön, biztonságosan tárolt többletinformáció

nélkül (többlépcsősen visszafejthető kapcsolati kód) ne lehessen azonosított vagy azonosítható személyhez rendelni. A Megbízott a kapcsolati kódon szimmetrikus és aszimmetrikus kulcsot hoz létre, amellyel titkosítják a személyes adatokat.

9.1.2. A rendszerek és szolgáltatások bizalmas jellege, integritása, rendelkezésre állása és ellenálló képessége: A Felek a hozzáférés ellenőrzése érdekében épületeiket az épületek biztonsági besorolása alapján, jól felépített beléptetési koncepcióban meghatározott beléptető rendszerrel védik. Biztonsági besorolástól függően az ingatlanok, épületek, illetve konkrét területek biztonságáról további intézkedésekkel is gondoskodnak. Ilyen intézkedések például a különleges hozzáférési profilok, a biometria, a személyi azonosító kódok (PIN) bevitelére szolgáló billentyűzetek, a DES hardverkulcsok, a külön belépési kódok, a video-kamerás megfigyelőrendszerek és az élőerős őrzés. Mindenki egyedileg kap hozzáférési jogosultságot, meghatározott feltételek alapján.

9.1.3. A rendszerhozzáférés ellenőrzése: A Felek adatkezelő rendszereihez kizárólag azok a hitelesített felhasználók férhetnek hozzá, akik a feladatkörük alapján erre felhatalmazást kaptak, a következő intézkedések mellett: az adatok titkosítása, (legalább 8 karakterből álló, rendszeres időközönként automatikusan lejáró) egyéni jelszó hozzárendelése, inaktivitás esetére jelszóval védett képernyővédők, behatolásjelző rendszerek és behatolásmegelőző rendszerek, rendszeresen frissített vírusvédők és kémprogramszűrők a hálózaton, valamint az egyes számítógépeken és mobileszközökön.

9.1.4. Az adatokhoz való hozzáférés ellenőrzésére: A Felek személyes adatokhoz hozzáférési jogosultságot feladatkörök szerinti engedélyezési rendszer szerint adnak. Olyan felhasználókezelő rendszert állítanak fel, amely a felhasználói adatbázishoz hozzárendeli a megfelelő jogosultságokat, és amelyből az adatkezelő rendszerek a hálózaton keresztül központilag kérhetnek le adatokat. Ezenkívül az adatok titkosítása megakadályozza a személyes adatokhoz való jogosulatlan hozzáférést.

9.1.5. Az adattovábbítás ellenőrzése: A Felek zárt hálózatok felállításával és adattitkosítási eljárásokkal védik az elektronikus kommunikációs csatornákat. Az adathordozók fizikai szállítása olyan ellenőrizhető szállítási folyamatok segítségével történik, amelyek megakadályozzák az adatokhoz való jogosulatlan hozzáférést, illetve a logikai veszteséget. Az adathordozókat az adatvédelmi rendelkezéseknek megfelelően vonják ki a forgalomból.

9.1.6. A rendszerek és szolgáltatások rendelkezésre állását és ellenálló képessége: A Felek úgy biztosítják a rendszerek és szolgáltatások rendelkezésre állását és ellenálló képességét, hogy a kulcsfontosságú informatikai és hálózati elemeket elszigetelik, gondoskodnak megfelelő biztonsági mentésről és redundanciáról, redundáns villamosenergia-rendszereket alkalmaznak, és rendszeresen tesztelik a rendszereket és szolgáltatásokat. A tesztrendszereket teljesen elkülönítik az éles rendszerektől.

9.1.7. A személyes adatok rendelkezésre állása és elérése incidensek esetén: A Felek a következő intézkedésekkel állítják helyre a személyes adatok rendelkezésre állását és elérhetőségét váratlan fizikai vagy technikai incidens esetén: a Felek biztonságos rendszerekben tárolják a személyes adatokat, a redundáns rendszereket pedig a biztonsági jelölés szerint integrálják. A Felek szünetmentes áramellátással (pl. szünetmentes tápegységgel, akkumulátorokkal, generátorokkal) biztosítják az adatközpontok áramellátását. A rendkívüli eseményekre a Felek átfogó, írásbeli vészhelyzeti tervet készítenek. A vészhelyzet esetén követendő eljárásokat és rendszereket rendszeres időközönként felülvizsgálják.

9.1.8. Az adatkezelés biztonsága érdekében végzett ellenőrzések: A Felek a kockázatkezelésen alapuló ellenőrzési eljárásokat alkalmaznak, figyelembe véve az Európai Unió és a székhelyük szerinti

ország informatikai hatóságainak alapvető informatikai védelmi előírásait, valamint az ISO/IEC 27001 szabvány előírásait, amelyek szerint az adatkezelés biztonsága érdekében a technikai és szervezési intézkedések hatékonyságát rendszeresen felül kell vizsgálni, fel kell mérni és értékelni kell. Ezzel biztosítható a lényeges információk, alkalmazások (köztük a minőség- és biztonságvizsgálati módszerek), az üzemi környezet (pl. a káros hatások kiszűrésére végzett hálózat monitorozás) védelme és a védelmi koncepciók műszaki kivitelezése (pl. sebezhetőségi elemzésekkel). A gyenge pontok szisztematikus felderítésével és elhárításával folyamatosan ellenőrzik és fejlesztik a védelmi intézkedéseket.

9.1.9. Személyügyi intézkedések: A Felek írásbeli utasításokat adnak ki és rendszeres képzésben részesítik a személyes adatokhoz hozzáférő munkavállalókat, annak érdekében, hogy a személyes adatok kezelése kizárólag a jogszabályok, és a jelen adatfeldolgozási szerződés szerint történjen.

10. Titoktartás: A Megbízott - a GDPR 28. cikke (3) bek b) pontjának megfelelően - biztosítja, hogy a személyes adatok kezelésére feljogosított személyek titoktartási kötelezettséget vállalnak, vagy jogszabályon alapuló megfelelő titoktartási kötelezettség alatt állnak és ezt igazolni tudja a Megbízó irányában.

11. Adatörlés: A Megbízott vállalja, hogy a vizsgálat elvégzésére irányuló megállapodásban rögzített vizsgálat befejezését követően - a GDPR 28. cikke (3) bek g) pontjának megfelelően - a Megbízó döntése alapján minden átvett, vagy adatfeldolgozóként kezelt személyes adatot töröl vagy visszajuttat a Megbízónak, és törli a meglévő másolatokat, kivéve, ha az uniós vagy a tagállami jog a személyes adatok tárolását írja elő. Az amennyiben az érintett a GDPR 17. cikk (1) b) pontjában rögzített jogával élve, az adatkezeléshez való hozzájárulását visszavonta úgy a Megbízott kötelezett arra, hogy az érintettnek az e célból kezelt adatait késedelem nélkül törölje.

12. Támogatás, monitoring, audit: A Megbízott vállalja továbbá, hogy az Alkalmazandó jogszabályokkal összhangban a Megbízó - a GDPR 28. cikke (3) bek h) pontjának megfelelően rendelkezésére bocsát minden olyan információt, amely kötelezettségei teljesítésének igazolásához szükséges, továbbá amely lehetővé teszi és elősegíti a Megbízó által végzett auditokat, beleértve a helyszíni vizsgálatokat is. A Megbízó tudomásul veszi, hogy csak és kizárólag a vizsgálatokkal kapcsolatos adatokba, rendszerekbe tekinthet be. A Megbízott szolgáltatói feladatai ellátásához kapcsolódó bármely személyes adatok kezelését végző rendszerhez, nyilvántartáshoz (pl. medikai rendszer) történő hozzáférése nem engedélyezett. Ennek keretében a Megbízott biztosítja a Megbízó képviselői a Megbízó és/vagy az illetékes egészségügyi hatóságok a jelen Megállapodás tartama alatt és azt követően is, munkaidőben, a Felek által előre egyeztetett észszerű időpontban ellenőrizzék:

a) azon létesítményeket, ahol a Szolgáltatásokat végzik,

b) a Szolgáltatások során létrehozott nyers vizsgálati adatokat; és

c) az egyéb releváns olyan információkat, amelyek szükségesek annak megállapításához, hogy azt alkalmazandó jogi és szabályozói követelményeknek megfelelően végzik-e, ideértve az adatvédelmi és adatbiztonsági jogszabályokat és előírásokat is.

13. A vizsgálat lefolytatásához használt berendezésekre, programokra, nyilvántartásokra, melyekkel adatkezelés valósul meg, vonatkozó rendelkezések

A Megbízó nyilatkozik és tudomásul veszi, hogy a megállapodásban foglaltakhoz biztosított berendezések, programok, nyilvántartások rendelkeznek mindazon biztonsági feltételekkel, melyekkel a személyes adatok megfelelő védelme biztosítható, továbbá, hogy ezek kiépítése, és

adatbevitel, -továbbítás, biztonsági feltételek ismertetése, esetleges betanítása a Megbízó feladata és kötelezettsége.

A vizsgálat elvégzésére irányuló megállapodás megszűnését követően a berendezések, programok, nyilvántartások visszaadása csak és kizárólag olyan módon történhet, amelynek során a személyes adatok védelme biztosított.

14. Adatvédelmi incidens bejelentése

Felek rögzítik, hogy az adatvédelmi incidensek során a GDPR-nak megfelelően járnak el jelen megállapodásban rögzítettek szerint. A Megbízott, mint adatfeldolgozó az adatvédelmi incidenst, az arról való tudomásszerzését követően indokolatlan késedelem nélkül, de legkésőbb 24 órán belül bejelenti a Megbízónak. Az értesítés folyamán a Megbízott – ha lehetséges – elegendő információt kell, hogy biztosítson a Megbízó számára ahhoz, hogy megtegye a szükséges intézkedéseket. Amennyiben a Felek mérlegelése alapján az adatvédelmi incidens valószínűsíthetően kockázattal jár a természetes személyek jogaira és szabadságaira, a Megbízott feladata gondoskodni arról, hogy indokolatlan késedelem nélkül, de legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, bejelentse azt az illetékes felügyeleti hatóságnak. Ha a bejelentés nem történik meg 72 órán belül, mellékelni kell hozzá a késedelem igazolására szolgáló indokokat is.

15. Az érintettek jogainak érvényesítése

15.1. Felek rögzítik, hogy amennyiben az érintett él a GDPR 15-22. cikkeiben meghatározott jogai érvényesítésével, akkor a Felek nevében a Megbízott jár el. Ha a Megbízó részére valamely érintett a GDPR 15-22. cikkeiben meghatározott jogai gyakorlása érdekében kérést küld, a Megbízó köteles továbbítani azt a Megbízottnak. Megbízott az alkalmazandó jogszabályoknak és a Megbízó egyéb utasításainak megfelelően válaszol az érintettek kéréseire. A Megbízó tudomásul veszi, hogy az érintettek bármikor visszavonhatják a hozzájárulásukat, azonban a hozzájárulás visszavonása nem érinti a hozzájáruláson alapuló, a visszavonás előtti adatkezelés jogszerűségét.

15.2. A Megbízott - a GDPR 28. cikke (3) bek. e) pontjának megfelelően - az adatkezelés jellegének figyelembevételével megfelelő technikai és szervezési intézkedésekkel a lehetséges mértékben segíti az adatkezelőt abban, hogy teljesíteni tudja kötelezettségét az érintettnek a GDPR III. fejezetében foglalt jogainak gyakorlásához kapcsolódó kérelmek megválaszolása tekintetében.

15.3. A Megbízott - a GDPR 28. cikke (3) bek. f) pontjának megfelelően segíti az adatkezelőt a GDPR 32–36. cikk szerinti kötelezettségek teljesítésében, figyelembe véve az adatkezelés jellegét és az adatfeldolgozó rendelkezésére álló információkat.

15.4. Az érintett GDPR 17. cikke (1) b) pontjában rögzített joga, hogy az amennyiben az adatkezeléshez való hozzájárulását visszavonta, adatait az adatkezelő törölje. Amennyiben az érintetett akár a Megbízó, akár a Megbízott felé ezen jogával él, úgy mind a Megbízó, mind a Megbízott kötelezett arra, hogy az érintettnek az e célból kezelt adatait késedelem nélkül törölje.

16. Adatfeldolgozók igénybe vétele

Felek rögzítik, hogy - a GDPR 28. cikkelyének (3) bek d) pontjának megfelelően - kizárólag olyan adatfeldolgozókat vehetnek igénybe, aki vagy amely megfelelő garanciát nyújt az adatkezelés Alkalmazandó jogszabályokban meghatározott követelményeinek való megfelelésre és az érintettek jogainak védelmét biztosító, megfelelő technikai és szervezési intézkedések végrehajtására. A Megbízott, mint adatfeldolgozó a Megbízó előzetesen írásban tett eseti vagy általános felhatalmazása nélkül további adatfeldolgozót nem vehet igénybe. Amennyiben a Megbízott önálló

adatkezelőként jár el, adatfeldolgozó igénybe vétele esetén a Megbízó engedélyét nem kötelező megkérnie.