

DENTALSINC • MAGYARORSZÁG

AVV/DPA – Adatfeldolgozási megállapodás

A GDPR 28. cikke szerinti megállapodás a DentalSyncben kezelt páciens-, eset- és szakmai adatokra

Dokumentumtípus Adatfeldolgozási megállapodás	Szolgáltató TOURMIX Hungary Kft.
Verzió 1.0	Utolsó frissítés 2026. május 29.

Szerződő felek: Adatkezelő/Ügyfél: a DentalSync szervezeti fiókjában azonosított rendelő vagy labor. Adatfeldolgozó: TOURMIX Hungary Kft. A megállapodás elektronikus elfogadással az adott szervezetre és az elfogadáskor rögzített dokumentumverzióra jön létre.

1. A megállapodás tárgya, hatálya és elsőbbsége

1.1. Jelen AVV/DPA a DentalSync B2B ÁSZF elválaszthatatlan adatfeldolgozási melléklete. A felek a GDPR 28. cikke alapján szabályozzák a személyes adatok Adatfeldolgozó általi, Adatkezelő nevében végzett kezelését.

1.2. Ha az Ügyfél maga is adatfeldolgozó – például valamely más adatkezelő dokumentált utasítása alapján használja a DentalSyncet –, az Adatfeldolgozó további adatfeldolgozóként jár el, és az Ügyfél garantálja, hogy rendelkezik a láncolt adatfeldolgozáshoz szükséges felhatalmazással.

1.3. Az Ügyfél szerződéses, kapcsolattartói, számlázási és fiókadminisztrációs adatai tekintetében a TOURMIX Hungary Kft. önálló adatkezelő; ezekre az adatkezelési tájékoztató vonatkozik. Jelen megállapodás a páciens-, eset-, klinikai, gyártási és szakmai kommunikációs adatokra alkalmazandó.

1.4. Adatvédelmi ellentmondás esetén az AVV/DPA elsőbbséget élvez az ÁSZF-fel szemben. A felek tényleges adatkezelési szerepét a valós működés határozza meg; a szerződés nem minősíthet önálló adatkezelést mesterségesen adatfeldolgozásnak.

2. A feldolgozás leírása

Elem	Tartalom
Tárgy	A DentalSync útján fogtechnikai esetek, munkalapok, fájlok, kommunikáció, partnerkapcsolatok, státuszok, határidők és

Elem	Tartalom
	kapcsolódó naplók fogadása, strukturálása, tárolása, megjelenítése, jogosult felek közötti továbbítása, mentése, exportja és törlése.
Cél	A rendelő és a labor közötti fogtechnikai munkafolyamat biztonságos, nyomon követhető és strukturált támogatása az Adatkezelő utasításai szerint.
Időtartam	A fő szerződés időtartama, az azt követő legfeljebb 30 napos exportidőszak és a mentések legfeljebb további 7 napos kifutása, kivéve kötelező jogszabályi megőrzés vagy dokumentált zárolás.
Műveletek	Gyűjtés, rögzítés, rendszerezés, strukturálás, tárolás, lekérdezés, megtekintés, jogosult címzettnek továbbítás, korlátozás, export, biztonsági mentés, törlés és anonimizálás.
Gyakoriság	Folyamatos, a Platform Ügyfél általi használatához igazodó.

3. Érintettek és adatkategóriák

Érintettek: páciensek – ideértve szükség szerint kiskorú páciens – , fogorvosok, fogtechnikusok, asszisztensek, rendelői és laboratóriumi munkatársak, szervezeti kapcsolattartók és futár-/átadási kapcsolattartók

Általános személyes adatok: belső páciens- vagy esetazonosító; kivételesen páciensnév; életkor vagy születési év, ha szakmailag szükséges; szervezeti és szakmai azonosítók; felhasználói név és elérhetőség; partnerkapcsolat; üzenet; fájlmetaadat; időpont; státusz; határidő; napló- és hozzáférési adat

Különleges személyes adatok: fogászati és egészségügyi adatok, kezelési információk, fogpozíció, fogszín, anyag, klinikai fotó, intraorális scan, STL és más digitális dentális fájl, fogtechnikai rendelvény és utasítás

Kifejezetten kerülendő adatok: TAJ-szám, lakcím, magántelefonszám, magán-e-mail, teljes születési dátum, pénzügyi vagy személyazonosító okmányadat, ha az adott munkafolyamat ezek nélkül is teljesíthető

3.1. Az Adatkezelő köteles a páciensadatokat minimalizálni és lehetőség szerint belső esetazonosítót használni. Az Adatfeldolgozó a Platform kialakításával támogatja, de nem tudja minden esetben önállóan megítélni a feltöltött adat szükségességét.

4. Az Adatkezelő jogai és kötelezettségei

- meghatározza az adatkezelés célját, jogalapját, az adatok körét, a címzetteket és a megőrzést;
- biztosítja a GDPR 6. és 9. cikke, az Eüak., valamint az egészségügyi és MDR-szabályok szerinti joglapot;
- az érintetteket átláthatóan tájékoztatja a DentalSync mint adatfeldolgozó igénybeviteléről és a rendelő–labor adattovábbításról;
- csak jogosult személynek ad hozzáférést, szerepköröket rendszeresen felülvizsgál, és a kilépő személy jogosultságát azonnal visszavonja;
- biztosítja a jogszerű partnerkapcsolatot, a fogtechnikai rendelvény pontosságát és a címzett labor megfelelő azonosítását;

- nem használja a Platformot az egyetlen kötelező egészségügyi vagy MDR-archívumként, és elvégzi a szükséges exportot;
- saját végpontjain, hálózatán, belső folyamataiban és felhasználóinál megfelelő biztonsági intézkedéseket alkalmaz;
- haladéktalanul tájékoztatja az Adatfeldolgozót a téves címeztről, jogellenes adatról, jogosultsági hibáról vagy incidensről.

4.1. Az Adatkezelő szavatolja, hogy utasítása jogszerű. Az Adatfeldolgozó nem köteles az Adatkezelő teljes jogi megfelelését előzetesen ellenőrizni, de jelzi, ha egy utasítás megítélése szerint sérti a GDPR-t vagy más adatvédelmi szabályt.

5. Dokumentált utasítások

5.1. Az Adatfeldolgozó személyes adatot kizárólag az ÁSZF, jelen AVV/DPA, az elfogadott Csomag, az Adatkezelő Platformon végzett művelete és írásbeli utasítása alapján dolgoz fel, kivéve ha uniós vagy magyar jog kötelező adatkezelést ír elő.

5.2. Kötelező jogszabályi adatkezelés előtt az Adatfeldolgozó tájékoztatja az Adatkezelőt, kivéve ha ezt fontos közérdekből jogszabály tiltja.

5.3. Az alapfunkciók körét meghaladó, jelentős fejlesztést, adat-helyreállítást vagy egyedi utasítást a felek külön egyeztetik; az Adatfeldolgozó a jogszabály szerint kötelező együttműködést nem teheti indokolatlan díjfizetéstől függővé.

5.4. Jogellenesnek tűnő utasítás végrehajtása a tisztázásig felfüggeszthető. Sürgős betegbiztonsági vagy adatvédelmi veszély esetén az Adatfeldolgozó a szükséges és arányos védelmi intézkedést önállóan is megteheti, majd dokumentáltan értesíti az Adatkezelőt.

6. Titoktartás és hozzáférő személyek

6.1. Az Adatfeldolgozó biztosítja, hogy a személyes adathoz hozzáférő munkavállaló, megbízott vagy közreműködő szerződéses vagy jogszabályi titoktartás alatt álljon, megfelelő adatvédelmi és biztonsági oktatást kapjon, és kizárólag feladatához szükséges hozzáféréssel rendelkezzen.

6.2. Éles páciensadathoz fejlesztői vagy support-hozzáférés csak dokumentált hibakezeléshez, időben korlátozottan, a legkisebb jogosultság elvével és naplózható módon engedhető. Supportjegybe, képernyőképbe vagy fejlesztői környezetbe egészségügyi adat nem másolható, ha anonimizált vagy mesterséges tesztadat elegendő.

7. Technikai és szervezési intézkedések

7.1. Az Adatfeldolgozó a kockázat, a technika állása, a megvalósítás költsége, az adat jellege és az érintettekre gyakorolt hatás figyelembevételével a GDPR 32. cikke szerinti intézkedéseket alkalmazza. A minimális intézkedéseket az 1. melléklet tartalmazza.

7.2. Az intézkedések a technikai fejlődéssel módosíthatók, ha a védelem összességében nem csökken. Lényeges, kockázatnövelő változásról az Adatkezelő előzetes tájékoztatást kap.

8. További adatfeldolgozók

8.1. Az Adatkezelő általános írásbeli felhatalmazást ad a 2. mellékletben felsorolt további adatfeldolgozók igénybevételére. Az Adatfeldolgozó minden további adatfeldolgozóval a GDPR 28. cikk (4) bekezdésének megfelelő, lényegében azonos védelmet biztosító megállapodást köt, és annak teljesítéséért a GDPR szerint felel.

8.2. Új vagy helyettesítő további adatfeldolgozóról – sürgős biztonsági vagy szolgáltatás-folytonossági eset kivételével – legalább 30 nappal korábban értesítést kell küldeni. Az Adatkezelő 15 napon belül dokumentált adatvédelmi okból tiltakozhat.

8.3. Megalapozott tiltakozás esetén a felek alternatívát keresnek. Ha észszerű alternatíva nem biztosítható, az Adatkezelő az érintett szolgáltatást a változás hatálybalépéséig felmondhatja, és adatait exportálhatja.

8.4. Scanner-, számlázási vagy futárintegráció, amelyet az Adatkezelő saját fiókjával és döntésével kapcsol össze, csak akkor minősül az Adatfeldolgozó további adatfeldolgozójának, ha azt a TOURMIX Hungary Kft. saját nevében vonja be. Közvetlen Ügyfél–harmadik fél kapcsolat esetén a harmadik fél az Adatkezelő címzettje vagy önálló adatfeldolgozója, amelyért az Adatkezelő felel.

9. Érintetti jogok és hatósági megkeresések

9.1. Az Adatfeldolgozó a kezelés jellegét figyelembe véve megfelelő technikai és szervezési intézkedéssel segíti az Adatkezelőt a hozzáférés, helyesbítés, törlés, korlátozás, adathordozhatóság és tiltakozás iránti kérelem teljesítésében.

9.2. Közvetlenül beérkező, Ügyfél által kezelt páciensadatra vonatkozó kérelmet az Adatfeldolgozó indokolatlan késedelem nélkül továbbít az illetékes Adatkezelőnek, és önállóan nem teljesít, kivéve jogszabályi kötelezettség vagy az Adatkezelő dokumentált utasítása alapján.

9.3. Hatósági vagy bírósági megkeresésről az Adatkezelőt – ha jogszerűen lehetséges – a teljesítés előtt értesíteni kell. Az Adatfeldolgozó csak a kötelező adatkört adja át, és a megkeresést, jogalapot, átadott adatkört és időpontot dokumentálja.

10. Adatvédelmi incidens

10.1. Az Adatfeldolgozó az Ügyféladatot érintő személyesadat-sértésről annak tudomására jutását követően indokolatlan késedelem nélkül, lehetőség szerint 24 órán belül értesíti az Adatkezelő kijelölt kapcsolattartóját.

10.2. Az első értesítés – az aktuálisan rendelkezésre álló mértékben – tartalmazza az esemény jellegét, időpontját, érintett rendszert, érintettek és adatok becsült körét, várható következményt, megtett vagy tervezett intézkedést és kapcsolattartót. Hiányzó információ részletekben is közölhető.

10.3. Az Adatfeldolgozó megőrzi a szükséges bizonyítékot, korlátozza a kárt, feltárja a kiváltó okot, együttműködik a 72 órás hatósági bejelentés és az érintetti tájékoztatás kockázatértékelésében. A bejelentés jogi kötelezettségéről az Adatkezelő dönt.

10.4. Az értesítés nem minősül felelősségelismerésnek. A felek incidensről csak a szükséges mértékben kommunikálnak nyilvánosan, figyelemmel az érintettek és a vizsgálat érdekeire.

11. Hatásvizsgálat, előzetes konzultáció és adatvédelmi tisztviselő

11.1. Az Adatfeldolgozó a rendelkezésére álló információval észszerűen segíti az Adatkezelőt a GDPR 32–36. cikke szerinti biztonsági kötelezettség, adatvédelmi hatásvizsgálat és előzetes konzultáció teljesítésében.

11.2. Mivel a Platform egészségügyi adatok több szervezet általi, strukturált kezelésére alkalmas, az Adatkezelő köteles indulás előtt dokumentált kockázatértékelést végezni, és megvizsgálni a DPIA, valamint a GDPR 37. cikke szerinti adatvédelmi tisztviselő kijelölésének szükségességét. Az Adatfeldolgozó saját kötelezettségét a szolgáltatás méretének és kockázatának változásakor rendszeresen felülvizsgálja.

12. Nemzetközi adattovábbítás

12.1. Az Adatfeldolgozó elsődlegesen EGT-beli tárolási régiót használ, ahol az adott szolgáltató ezt biztosítja. Éles páciensfájlok Backblaze-tárolására kizárólag az EU Central (Amszterdam) régió használható.

12.2. EGT-n kívüli szervezet általi távoli hozzáférés vagy továbbítás csak a GDPR V. fejezete szerinti jogalappal – különösen megfelelőségi határozat, EU–USA adatvédelmi keretben fennálló érvényes tanúsítás vagy a 2021/914/EU határozat szerinti általános szerződési feltétel – és szükség esetén kiegészítő intézkedéssel történhet.

12.3. Az Adatfeldolgozó nyilvántartja a tényleges régiót, a címzettet, továbbítási mechanizmust és kockázatértékelést. A mechanizmus érvénytelenné válásakor haladéktalanul alternatívát alkalmaz, felfüggeszti az érintett továbbítást vagy értesíti az Adatkezelőt.

13. Adatvisszaadás, export, törlés és megőrzés

13.1. A fő szerződés alatt az Adatkezelő a Platform funkcióin keresztül jogosult saját adatainak elérésére, helyesbítésére, letöltésére és – a szakmai, jogi és partneri kötelezettségekre figyelemmel – törlésére.

13.2. Megszűnéskor az Adatkezelő választása szerint az Adatfeldolgozó a személyes adatot visszaadja/exportálhatóvá teszi, majd törli, vagy közvetlenül törli. eltérő utasítás hiányában 30 napos exportidőszak után az aktív rendszerekből törlés vagy visszafordíthatatlan anonimizálás történik.

13.3. Napi adatbázis-snapshot legfeljebb hét napig marad fenn. Ezalatt a mentés elkülönítetten, kizárólag helyreállítási célra kezelhető, majd automatikusan felülíródik. A fájl tárolás aktív példányának törlését az Adatfeldolgozó kezdeményezi; a szolgáltatói technikai másolat kizárólag a szolgáltatói DPA szerinti, védett kifutási időben maradhat fenn.

13.4. Jogszabály alapján tovább megőrzendő adatot az Adatfeldolgozó zárolja, más célra nem használja, és a kötelező idő végén törli. A zárolás okáról és köréről az Adatkezelőt tájékoztatja.

14. Ellenőrzés és megfelelés igazolása

14.1. Az Adatfeldolgozó rendelkezésre bocsátja a GDPR 28. cikkének való megfeleléshez szükséges észszerű információt, így különösen jelen AVV/DPA-t, az intézkedések összefoglalóját, alfeldolgozói listát és elérhető független tanúsítást vagy auditösszefoglalót.

14.2. Az Adatkezelő évente egyszer, legalább 30 napos értesítéssel dokumentumalapú auditot kezdeményezhet. Helyszíni vagy technikai audit csak akkor kérhető, ha a dokumentumalapú ellenőrzés nem elegendő, vagy incidens, hatósági megkeresés, illetve megalapozott súlyos hiányosság indokolja.

14.3. Az audit nem veszélyeztetheti más ügyfelek adatait, a Platform biztonságát, üzleti titkot vagy szolgáltatásfolytonosságot. Független, titoktartásra köteles auditor alkalmazandó. A szokásos igazolás az alapidj része; aránytalan egyedi vizsgálat indokolt többletköltsége előzetes egyeztetés alapján áthárítható.

15. Felelősség, időtartam és megszűnés

15.1. A felek a GDPR szerint saját kötelezettségeikért felelnek. Jelen AVV/DPA nem korlátozza az érintett közvetlen jogait, a felügyeleti hatóság hatáskörét vagy a GDPR alapján kötelező felelősséget.

15.2. Az AVV/DPA a fő szerződéssel lép hatályba, és addig marad alkalmazandó, amíg az Adatfeldolgozó az Ügyfél nevében személyes adatot kezel, ideértve az export- és törlési időszakot.

15.3. A fő szerződés megszűnésekor az adatkezelési rendelkezések az adat teljes törléséig, a titoktartás pedig időbeli korlátozás nélkül fennmarad.

1. melléklet – Minimális technikai és szervezési intézkedések

Kontrollterület	Minimális intézkedés
Irányítás és kockázat	Dokumentált adatvédelmi és információbiztonsági felelősség; rendszeres kockázatértékelés; változáskezelés; beszállítói átvilágítás; incidens- és helyreállítási eljárás.
Hozzáférés-kezelés	Egyedi felhasználói fiók; szerepköralapú legkisebb jogosultság; adminjog korlátozása; belépő–módosuló–kilépő folyamat; hozzáférések rendszeres felülvizsgálata; megosztott fiók tiltása.
Hitelesítés	Biztonságosan hashelt jelszó; erős jelszókövetelmény; reset token és munkamenet automatikus lejárat; brute-force elleni védelem; többtényezős hitelesítés alkalmazása, amint a produkciós funkció ezt támogatja, adminoknál elsőbbséggel.
Átvitel és tárolás	TLS/HTTPS a támogatott végpontok között; privát fájl tárolás; szolgáltatói hozzáférés-védelem; nyugalmi titkosítás alkalmazása a produkciós infrastruktúrában; titkok elkülönített kezelése és rendszeres cseréje.

Kontrollterület	Minimális intézkedés
Adattakarékosság	Belső esetazonosító támogatása; TAJ és szükségtelen közvetlen azonosító kerülése; generikus e-mail-értesítés; tesztkörnyezetben mesterséges vagy anonimizált adat.
Naplózás	Belépés, sikertelen próbálkozás, adminművelet, partnerkapcsolat, dokumentumelfogadás, lényeges adat- és jogosultságváltozás arányos naplózása; naplóhozzáférés korlátozása; időszinkron.
Fejlesztés és sebezhetőség	Kódhozzáférés korlátozása; felülvizsgált deploy; függőségek és biztonsági frissítések kezelése; sérülékenység-bejelentési csatorna; titok és éles adat kizárása a forráskódból.
Mentés és helyreállítás	Napi adatbázis-snapshot, legfeljebb 7 napos gördülő megőrzéssel; jogosultságvédelem; dokumentált és rendszeresen tesztelt visszaállítás; helyreállítás eseménynaplózása.
Incidenskezelés	Észlelés, belső eskaláció, kárkorlátozás, bizonyítékmegőrzés, okfeltárás, ügyfélértesítés, javító intézkedés és utóellenőrzés.
Törlés és hordozhatóság	Szerződés alatti törlési funkciók; 30 napos export; aktív adatok dokumentált törlése; mentések automatikus kifutása; jogi zárolás elkülönítése.
Fizikai és környezeti védelem	A felhő- és tárhelyszolgáltatók adatközponti fizikai, energiaellátási, tűz-, belépési és környezeti kontrolljainak szerződéses igénybevétele és rendszeres felülvizsgálata.
Elérhetőség és elkülönítés	Ügyfélszervezetek logikai elkülönítése; hibás objektum-hozzáférés elleni kontroll; kapacitásfigyelés; karbantartás; üzletmenet-folytonossági és vészhelyzeti eljárás.

2. melléklet – Jóváhagyott további adatfeldolgozók

Kötelező produkciós beállítás: Éles páciensfájl csak Backblaze EU Central (Amszterdam) régióban tárolható. A Laravel Cloud tényleges projekt-/adatbázis-régióját és a szerződéses adattovábbítási mechanizmust az indulási jegyzőkönyvben rögzíteni kell. SendGrid-üzenet tárgya és törzse nem tartalmazhat páciensnevet, esetazonosítót, diagnózist, képet, fogászati utasítást vagy más egészségügyi adatot.

Szolgáltató	Feladat	Adatkör	Hely / garancia
Laravel Holdings Inc. – Laravel Cloud	alkalmazás- és adatbázis-hosting, futtatókönyezet, technikai napló, napi adatbázis-snapshot	felhasználói, szervezeti, eset-, kommunikációs és klinikai adatok a szükséges mértékben	a produkciós projektben kiválasztott régió; EGT-n kívüli hozzáférés esetén GDPR V. fejezet szerinti garancia
Backblaze, Inc. – Backblaze B2	feltöltött képek, scanek, STL és más fájlok objektumtárolása	fájl tartalma és technikai metaadata; különleges adatot is tartalmazhat	EU Central régió, Amszterdam; amerikai szolgáltatói hozzáférés esetén érvényes DPF/SCC és szükséges kiegészítő intézkedés
Twilio Inc. / szerződő Twilio-entitás – Twilio SendGrid	tranzakciós, generikus rendszerértesítés és kézbesítési státusz	felhasználói e-mail-cím, generikus tárgy/törzs, feladó, időpont, kézbesítési metaadat; egészségügyi adat tilos	globális szolgáltatási infrastruktúra; EGT-n kívüli továbbításnál DPF és/vagy 2021/914/EU SCC a szolgáltatói DPA szerint

3. melléklet – Incidens- és adatvédelmi kapcsolattartás

Adatfeldolgozó kapcsolattartója: admin@dentalsync.eu

Adatkezelő kapcsolattartója: a szervezeti fiókban megjelölt adminisztrátori/adatvédelmi e-mail-cím

A szervezeti adminisztrátor köteles az incidens- és adatvédelmi kapcsolattartót naprakészen tartani. Ha az Adatkezelő adatvédelmi tisztviselőt jelölt ki, annak elérhetőségét a fiókban külön rögzíti.

Főbb jogszabályi és szakmai hivatkozások

- GDPR – különösen 28., 32–36. és 44–49. cikk: <https://eur-lex.europa.eu/eli/reg/2016/679/oj/hun>
- EDPB 07/2020 iránymutatás az adatkezelő és adatfeldolgozó fogalmáról: https://www.edpb.europa.eu/system/files/2023-10/EDPB_guidelines_202007_controllerprocessor_final_en.pdf
- 2021/915/EU adatkezelő–adatfeldolgozó mintakikötések: https://eur-lex.europa.eu/eli/dec_impl/2021/915/oj
- NAIH adatvédelmi hatásvizsgálati lista: <https://www.naih.hu/hatasvizsgalati-lista>
- Backblaze EU-régiók: <https://www.backblaze.com/docs/cloud-storage-data-regions>
- Twilio Data Protection Addendum: <https://www.twilio.com/en-us/legal/data-protection-addendum>