Adatfeldolgozói Megállapodás (Data Processing Agreement — DPA)

Dokumentum azonosítója: SURWAYR-DPA-v1.1

Utoljára frissítve: 2026. március 28.

Ez a megállapodás a **Devtronics Kft. (SURWAY'R)** mint adatfeldolgozó (a továbbiakban: „Adatfeldolgozó") és a **Felhasználó** mint adatkezelő (a továbbiakban: „Adatkezelő") között jön létre a Szolgáltatás használatával automatikusan, külön aláírás nélkül.

Az általános DPA-feltételek a Szolgáltatás regisztrációjával és az ÁSZF elfogadásával automatikusan elfogadottnak minősülnek. Amennyiben szervezete **külön, aláírt DPA-megállapodást** igényel, kérheti azt a legal@surwayr.com e-mail-címen (legalább Team előfizetési szinthez kötött).

A jelen DPA-ban a „személyes adat", „adatkezelő", „adatfeldolgozó", „érintett", „adatkezelés", „adatvédelmi incidens" fogalmak a GDPR (EU) 2016/679 rendeletben, illetve az alkalmazandó európai adatvédelmi jogszabályokban meghatározott értelmet hordozzák.

---

1. Tárgy, tartalom és adatkezelési kontextus

A Felhasználó a kérdőívplatformon keresztül személyes adatokat gyűjt és kezel. Az Adatfeldolgozó ezen adatok tárolását, strukturálását, elemzését és az Adatkezelő számára való rendelkezésre bocsátását végzi, kizárólag az Adatkezelő utasításai szerint.

Az adatkezelés főbb jellemzői: - **Időtartam:** A felek közötti szerződéses jogviszony fennállásáig, illetve az Adatkezelő fiókjának törléséig - **Jelleg:** Adatgyűjtés, tárolás, szervezés, hosting, az adatok Adatkezelő részére való hozzáférhetővé tétele, törlés - **Cél:** Kérdőív-alapú adatgyűjtés, tárolás és elemzési eszközök biztosítása az Adatkezelő részére - **Érintett személyek típusai:** Az Adatkezelő kérdőíveire válaszoló személyek (válaszadók), az Adatkezelő szervezetének tagjai - **Személyes adatok kategóriái:** Név, e-mail-cím, telefonszám, egyéb azonosítók, az Adatkezelő kérdőíveibe beépített egyéb adatok — beleértve esetlegesen különleges kategóriájú adatokat, amelyek kezeléséért az Adatkezelő vállalja a kizárólagos felelősséget

---

2. Az Adatfeldolgozó kötelezettségei

Az Adatfeldolgozó vállalja, hogy:

- Csak az Adatkezelő dokumentált utasításai alapján kezeli az adatokat. „Dokumentált utasítás" alatt a következők értendők: (i) tartós adathordozón (levél, e-mail) közölt utasítás; (ii) a Szolgáltatás szoftverfelületén keresztül elektronikusan megadott utasítás; (iii) jelen DPA rendelkezései.
- Ha az Adatfeldolgozónak alapos oka van feltételezni, hogy egy utasítás sérti a GDPR-t vagy más alkalmazandó adatvédelmi jogszabályt, az utasítást felfüggeszti és haladéktalanul értesíti az Adatkezelőt. Az Adatkezelő kizárólagos kockázatára és felelősségére az utasítást írásban megerősítheti, ebben az esetben az Adatfeldolgozó végrehajtja azt.
- Biztosítja a titoktartási kötelezettséget az adatokhoz hozzáférő összes munkavállalója és alvállalkozója részéről — szerződéses, illetve törvényi titoktartási kötelezettség alapján.

- Az adatokat kizárólag a jelen DPA-ban meghatározott célokra használja; harmadik félnek kizárólag a jelen DPA-ban engedélyezett módon adja át.
- Uniós vagy tagállami jog által előírt adatkezelés esetén (beleértve a személyes adatok nemzetközi továbbítását) — hacsak azt közérdekből jogszabály nem zárja ki — az adatkezelés előtt értesíti az Adatkezelőt.

---

3. Al-adatfeldolgozók

Az Adatkezelő a Szolgáltatás igénybevételével általánosan hozzájárul az alábbi al-adatfeldolgozók igénybevételéhez:

Al-adatfeldolgozó	**Tevékenység**	**Székhely**	**Adattovábbítás jogalapja**
Hetzner Online GmbH	Infrastruktúra, tárhely	Németország (EU)	EGT-n belül, nincs szükség SCC-re
Stripe Ireland Limited	Fizetésfeldolgozás	Írország (EU)	EGT-n belül
Resend Inc.	Tranzakciós e-mailek	USA	SCC (2021/914/EU modul 2)
Google LLC (Gemini API)	AI elemzés (opcionális, Gemini modell)	USA	SCC (2021/914/EU modul 2)
Groq, Inc.	AI elemzés (opcionális, LLM következtetés)	USA	SCC (2021/914/EU modul 2)

Ha az Adatfeldolgozó **új al-adatfeldolgozót kíván igénybe venni vagy meglévőt lecserélni**, erről az Adatkezelőt legalább **15 naptári nappal** előre értesíti (e-mailben a regisztrált e-mail-címre, vagy a Szolgáltatáson belüli értesítésben). Az Adatkezelő ezen határidőn belül **indokolt kifogást** emelhet (a kifogás kizárólag olyan okból érvényes, ha az al-adatfeldolgozó nyilvánvalóan nem teljesíti a GDPR által megkövetelt garanciákat). Ha az Adatkezelő él kifogásolási jogával, az Adatfeldolgozó jogosult a szolgáltatási szerződést előzetesen, 30 napos felmondási idővel megszüntetni.

Az Adatfeldolgozó minden al-adatfeldolgozóval írásba foglalt megállapodást köt, amely a GDPR által megkövetelt garanciákat és biztosítékokat tartalmazza. Az Adatfeldolgozó az al-adatfeldolgozók magatartásáért mint sajátjáért felel az Adatkezelő felé.

---

4. Érintetti jogok

Az Adatfeldolgozó — az adatkezelés természetéhez és a rendelkezésre álló információkhoz mérten — megfelelő technikai és szervezési intézkedésekkel segíti az Adatkezelőt a GDPR III. fejezete szerinti érintetti jogok (hozzáférés, helyesbítés, törlés, korlátozás, adathordozhatóság, tiltakozás) teljesítésében.

Ha bármely érintett az Adatfeldolgozóhoz fordul jogai gyakorlása céljából, az Adatfeldolgozó haladéktalanul, de legkésőbb **5 munkanapon belül** továbbítja a kérelmet és a kapcsolódó összes információt az Adatkezelőnek. Az érintettet tájékoztatja arról, hogy az Adatkezelő felelős a válaszadásért.

---

5. Technikai és szervezési biztonsági intézkedések

Az Adatfeldolgozó az adatkezelés kockázatának megfelelő szintű biztonságot biztosít az alábbi főbb intézkedések révén:

Hálózati biztonság: - Hozzáférés-kezelési és adattovábbítási szabályzatok, hitelesítési mechanizmusok, tűzfal és behatolásészlelő rendszerek - Biztonsági incidensek kezelésére vonatkozó eljárásrend (Incident Response Plan)

Fizikai biztonság: - A fizikai infrastruktúra ISO 27001 tanúsítvánnyal rendelkező adatközpontban (Hetzner) üzemel, vagy azzal egyenértékű fizikai biztonsági követelményeket teljesítő létesítményben; a fizikai hozzáférés az üzleti szükséglet alapján korlátozott

Személyes adatok biztonsága: - Adatok titkosítása átvitel közben (TLS 1.2 vagy magasabb) és tároláskor (AES-256) - Adatminimalizálás, célhoz kötöttség és alapértelmezett adatvédelem elvének alkalmazása - Rendszeres biztonsági tesztelés és értékelés - Hozzáférés-kontroll és szerepköralapú jogosultságkezelés (RBAC) - Kétfaktoros hitelesítés (2FA) az adminisztrációs hozzáférésekhez - Rendszeres biztonsági tudatossági képzés az érintett munkavállalóknak

Üzletmenet-folytonosság: - Üzletmenet-folytonossági és katasztrófa-utáni helyreállítási terv, amelyet évente legalább egyszer tesztelnek - Biztonsági mentések (backup) legfeljebb **90 napig** őrzendők meg

Titoktartás: - Az adatokhoz hozzáférő munkavállalók és alvállalkozók titoktartási megállapodással kötöttek

Consent audit-napló (Jogi hozzájárulás naplózás): - Az Adatfeldolgozó a felhasználói hozzájárulásokat egy **tamper-resistant, append-only** rendszerben rögzíti: az adatbázis-rétegen adatbázis-trigger akadályozza a rekordok utólagos módosítását vagy törlését; a naplófájl-rétegen SHA-256 hash-lánc biztosítja a sértetlenség igazolhatóságát. - Ez a rétegelt rendszer bizonyítható, ellenőrizhető igazolást nyújt a hozzájárulás megtörténtéről, annak körülményeiről és az elfogadott dokumentumok verziószámairól.

Az Adatfeldolgozó rendszeres időközönként felülvizsgálja és szükség szerint frissíti a biztonsági intézkedéseket, és nem csökkenti azok összesített szintjét az Adatkezelő értesítése nélkül.

---

6. Incidenskezelés és bejelentés

Az Adatfeldolgozó haladéktalanul, de legkésőbb **72 órán belül** értesíti az Adatkezelőt, miután tudomást szerzett az érintett személyes adatokat érintő adatvédelmi incidensről. Az értesítés tartalmazza legalább: az incidens körülményeinek leírását; az érintett személyek és adatkategóriák hozzávetőleges számát; az incidens valószínűsíthető következményeit; az Adatfeldolgozó által tett vagy tervezett intézkedéseket.

Az Adatfeldolgozó a rendelkezésre álló információk alapján ésszerű kereskedelmi erőfeszítéseket tesz az Adatkezelővel együttműködve az incidens kivizsgálása, enyhítése és megszüntetése érdekében.

Az Adatkezelő kizárólagosan felelős az alkalmazandó jogszabály által előírt hatósági bejelentések megtételéért (pl. NAIH) és az érintett személyek tájékoztatásáért. Az Adatkezelő megvédi, kártalanítja és mentesíti az Adatfeldolgozót minden olyan igény, veszteség és költség alól, amely az Adatkezelő mulasztásából vagy késedelméből ered.

---

7. Az adatok törlése vagy visszaszolgáltatása

Az Adatkezelő dönt arról, hogy a szerződés megszűnésekor az Adatfeldolgozó törölje vagy visszaszolgáltassa a személyes adatokat, kivéve ha uniós vagy tagállami jog az adatok megőrzését írja elő.

A fiók törlése az Adatkezelő részéről a 7. szakasz szerinti adattörlési kérelem bejelentéseként értelmezendő. A biztonsági mentések (backup) legfeljebb **90 napon belül** törlésre kerülnek a szerződés megszűnését követően.

> **Kivétel — Consent audit-naplók:** A jogi hozzájárulási audit-naplók (`legal_consent_events` adatbázis-rekordok és a `legal.log` hash-lánc) a fiók megszűnésétől számított **5 évig** megőrzésre kerülnek. Ennek jogalapja a Szolgáltató jogos érdeke (GDPR 6(1)(f)): az esetleges jogviták kezelési képességének biztosítása a polgári jogi elévülési idő figyelembevételével. Ezek az adatok nem tartalmazzák a kérdőív-tartalmakat vagy válaszadói adatokat; kizárólag az elfogadási esemény tényét, időbélyegét, dokumentumverzióit, IP-cím- és user-agent-adatokat rögzítik.

A fizetős előfizetés lemondása (de a fiók fenntartása mellett) nem eredményezi a jelen DPA megszűnését; az Adatkezelő az ingyenes csomagban folytathatja a Szolgáltatás használatát.

---

8. Auditálási jogok

Az Adatfeldolgozó rendelkezésre bocsátja a jelen DPA szerinti kötelezettségek teljesítésének igazolásához szükséges dokumentumokat. Az Adatkezelő elsősorban a vonatkozó audit-jelentések és tanúsítványok (pl. ISO 27001, SOC 2) másolatainak megküldésével elégíti ki az auditálási igényt.

Ha ezek a dokumentumok nem elégítik ki az Adatkezelő ésszerű aggályait, az Adatkezelő évente legfeljebb **1 auditot** végezhet (kivéve ha alapos okkal feltételezi a DPA lényeges megsértését). Az auditot rendes munkaidőben kell lefolytatni; az Adatkezelő viseli az audit összes költségét, kivéve ha az audit a DPA lényeges megsértését tárja fel, amely esetben az Adatfeldolgozó viseli a tényleges auditköltségeket.

---

9. Személyes adatok nemzetközi továbbítása

Az EGT-n kívüli (különösen USA-ba irányuló) adattovábbítás jogalapja az Európai Bizottság 2021/914/EU végrehajtási határozata alapján elfogadott **Standard Contractual Clauses (SCC)**, amelyeket az al-adatfeldolgozókkal kötött szerződéseink tartalmazzák.

Igénybe vett modulok: - **2. modul** (Controller → Processor): Resend, Google LLC (Gemini), Groq esetén

A vonatkozó SCC-k másolatát az Adatkezelő kérésére rendelkezésre bocsátjuk (privacy@surwayr.com).

Transfer Impact Assessment (TIA): Az USA-ba irányuló adattovábbítás kapcsán elvégzett hatásvizsgálatok dokumentálva elérhetők belső jogi iratanyagunkban. A Google Gemini és Groq API esetén a kérdőív-tartalom adatminimalizált formában kerül az AI API-khoz; személyes azonosítókat (névmel, e-mail-cím) nem adunk át.

---

10. Enterprise / egyedi aláírt DPA

Az általános DPA-feltételek a Szolgáltatás használatával automatikusan elfogadottnak minősülnek. Ha szervezete külön, aláírt DPA-megállapodást igényel (pl. belső megfelelési követelmények, közbeszerzési előírások, egészségügyi vagy pénzügyi szabályozói elvárások miatt), kérheti azt a legal@surwayr.com e-mail-címen.

- Az egyedi DPA alapja jelen dokumentum; a tárgyalható elemek az adatmegőrzési időszakok, az audit-jogosultságok és az al-adatfeldolgozói értesítési határidők.
- Az egyedi DPA aláírása legalább **Team** előfizetési szinthez kötött.
- A Szolgáltató az igény kézhezvételétől számított **10 munkanapon belül** visszajelez.