

## Adatfeldolgozói tájékoztató

Jelen leírással célunk, hogy tájékoztatást adjunk Ügyfeink számára cégünk, a Dankó István E.V. tárhely szolgáltató szervezet tárhelyszolgáltatási, a GDPR alapján adatfeldolgozói tevékenységéről. [GDPR: Európai Parlament és a Tanács (EU) 2016/679 rendelete]

A tárhely szolgáltatás használata során a tárhelyre adatok tölthetők fel, melyek egy része személyes adatnak minősül. Az adatkezelő feladata, hogy ezeknek az adatoknak a kezelése a GDPR-nek megfelelően történjen. A tárhelyen a weboldal megjelenítését biztosító programkódot és az adatok tárolási módját (pl. álnevesített formáját) Előfizető maga választja meg. Adatfeldolgozóként cégünk az adatokhoz kapcsolódóan a tárolás és mentés technikai műveletét biztosítja, a további adatkezelési műveleteket az Adatkezelő végzi.

A cégunktől bérelt tárhelyre feltöltött adatok, köztük a személyes adatok védelme érdekében cégünk több adminisztratív és műszaki lépéssel segíti az adatkezelő tevékenységét:

**Kapcsolattartó:** a tárhely előfizetés során az Előfizető egy vagy több személyt jelölhet meg cégünk felé kapcsolattartóként. A kapcsolattartó részére küldjük valamennyi értesítésünket a szolgáltatással kapcsolatban, továbbá ez a személy fér hozzá megadott email címe vagy az arra küldött üzenetek segítségével rendszereinkhez.

**Ügyfélkapu:** a műszaki beállítások kezeléséhez kialakított, egyedi fejlesztésű, központi rendszer. A tárhely előfizetés aktiválását követően a Kapcsolattartó megkapja e-mailben az azonosító és jelszó párost, amellyel a rendszerhez hozzáfér. Javasoljuk az első belépést követően a jelszó megváltoztatását úgy, hogy az ne egyezzen meg máshol használt jelszóval. Nem javasoljuk, hogy a kapcsolattartó a számára átadott Ügyfélkapu azonosítót és jelszót a megjelölt kapcsolattartókon kívül más félnek átadja, amennyiben ez mégis szükséges (pl. weboldal készítő részére), javasolt az Előfizető részéről a hozzáférésre jogosultakról saját nyilvántartás vezetése.

**FTP:** az FTP hozzáférési azonosító és jelszó megegyezik az Ügyfélkapu azonosítóval és jelszóval. A tárhelyre feltöltött fájlokat FTP kapcsolaton keresztül lehet elérni kliens programokkal. Javasoljuk biztonságos kliens program választását a csatlakozásra.

**FTP kapu védelem:** alapértelmezetten az FTP-re történő csatlakozás előtt a kliens számítógép IP címének hitelesítésére van szükség annak érdekében, hogy a tárhelyen megtalálható fájlokhoz FTP-vel hozzá lehessen férni. Ez a védelem esetlegesen bekövetkező jelszólopás esetén nyújt segítséget, meggátolva az illetéktelen (nem hitelesített) IP címről történő hozzáférést.

**MySQL adatbázis elérése:** a tárhelyekhez tartozó adatbázisok alapértelmezetten kizárólag a helyi szerverről (localhost) érhetők el. Van lehetőség külső mysql kapcsolódás aktiválására, külön megrendelés esetén, ebben az esetben javasolt fix IP címet megadni, ahonnan a csatlakozás történik. Az adatbázis az Ügyfélkapu hozzáférési adataitól különálló azonosítóval és jelszóval hozzáférhető.

**Szerverek elhelyezése:** a tárhelyeket kiszolgáló szervereken lévő adatokhoz kizárólag cégünk rendszergazdái férnek hozzá. A szerverek fizikailag Corvus Kft telephelyén, szerverteremben kerülnek elhelyezésre.

**Online Ügyfélszolgálat:** az Előfizető adatainak és szolgáltatásainak áttekintésére, módosítására szolgáló adminisztrációs felület. Lehetőséget biztosít Kapcsolattartó változtatásra, amely módosítás papír alapú, aláírással hitelesített dokumentum benyújtásával is megtehető.

**Jelszóváltoztatás:** az Ügyfélkapu és az Online Ügyfélszolgálat felületéhez történő hozzáférési jelszó bármikor megváltoztatható, ezt javasoljuk rendszeres időközönként megtenni. Az aktuális jelszó ismeretében erre mindkét felület lehetőséget biztosít. Elfelejtett jelszó esetén az Előfizető az előzetesen megadott kapcsolattartói email címére kérhet jelszó emlékeztető e-mailt, az ebben található jelszó változtató link segítségével adhat meg új jelszót. A jelszó változtatás tényét naplózzuk.

**Napi mentés:** a tárhelyre feltöltött adatokról rendszeres biztonsági mentést készítünk, amely díjmentesen letölthető az Ügyfélkapu felületéről. Ez abban az esetben lehet hasznos, ha az adatkezelőnek az adatok visszaállítására van szüksége. Az adatmentések korlátozott ideig érhetők el, azonban felhívjuk a figyelmet az Általános Szerződési Feltételeinkben is szereplő kitételekre, mely szerint a mentésre vonatkozóan garanciát, vagy az adatvesztésből eredő károkért felelősséget nem vállalunk. A GDPR értelmében az adatkezelő felelőssége a visszaállíthatóság biztosítása. Előfizetőinknek javasoljuk a szerveren tárolt állományok rendszeres, saját eszközre történő mentését.

**Tárhelyre telepített programok biztonsági rései:** az Előfizető a saját választása szerinti weboldal programkódot tölti fel a tárhelyre. Ezeknek a programkódoknak a rendszeres, naprakész frissítése kritikus fontosságú az adatvédelem szempontjából, ugyanis a biztonsági réseken keresztül illetéktelenek hozzáférhetnek a tárhelyre feltöltött adatokhoz. Fontos, hogy ilyenkor nem a weboldal technikai működését biztosító szerveret törlik fel, hanem a weboldal biztonsági réseit kihasználva az adott tárhelyen található weboldal fájljaihoz és azon keresztül az adatbázisához férnek hozzá. Különösen fontos az ún. nyílt forráskódú rendszerek (pl. Joomla, WordPress) vagy az azokhoz telepített bővítmények frissítése, mivel ezekben a kódokban bárki kereshet és találhat biztonsági rést. Ezeket a réseket a nyílt forráskódú keretrendszer fejlesztői általában javítják, de a tárhelyen található programkód frissítése az Előfizető feladata. Elavult program vagy bővítmény használata nem javasolt, ugyanis a biztonsági réseket robot programok segítségével kihasználhatják a weboldal feltörésére.

**Titkosított, https:// elérés:** a weboldal a böngészőkben a http:// elérés mellett https:// protokollal is elérhető. Utóbbi lényegében egy titkosított csatornát jelent a böngésző és a webszerver között. A https:// protokoll aktiválásához szükség van egy SSL kulcsra. Ilyen kulcsot egyrészt díjmentesen tudunk biztosítani Ügyfeleink részére az Internet Security Research Group által (let's encrypt), vagy lehetőség van külső szolgáltatók által kiállított SSL tanúsítvány használatára is (Digicert, Comodo stb...) Mindazonáltal fenntartjuk a jogot a díjmentes szolgáltatás feltételeinek megváltoztatására, és nem vállalunk felelősséget a továbbadott szolgáltatással kapcsolatban felmerülő hibákért. A díjmentes kulcs és a szolgáltatás az Ügyfélkapu felületén aktiválható. A tárhelyre telepített programkódban szükséges módosításokat végrehajtani a https használatához.

**E-mail szolgáltatás:** a regisztrált domain nevekhez igénybe vehető email szolgáltatás, amely az értékesített díjcsomagok részét képezi. Az email címekhez a postafiók létrehozása során megadott jelszóval lehet hozzáférni. Javasoljuk a jelszó rendszeres időközönként történő megváltoztatását.

**Spam és víruszűrés:** az email címekre érkező levelek - bekapcsolt szűrés esetén - ellenőrzésen esnek át. A szűrés pontszám alapú rendszerben történik, a ponthatárok a Postafiók beállításai között változtathatók. A megfelelő védelem érdekében erősen javasolt csak az ismerős feladóktól érkező levelek és mellékletek megnyitása, és a bizonytalan forrásból származó levelek és mellékletek törlése, mert utóbbiak tartalmazhatnak olyan vírust, amelyet az általunk is használt nagyvállalati rendszerek (Cloudmark, Clamav) még nem érzékelnek. A szűrők nem elemzik, nem tárolják, nem továbbítják a levelek tartalmát, csak az ismert és heurisztikus minták alapján keres bennük vírus és spamgyanús mintákat.

**POP3S és IMAPS:** levelező program (pl. Outlook, Thunderbird) használata esetén elérhető titkosított csatlakozási mód a kliens és a szerver között. Javasolt a beállítások során ezt igénybe venni. Cégünk a levelek elérésére a <https://mail.tarhely-ozd.hu/webmail/> címen biztosít webes, titkosított kapcsolattal lehetőséget.

**Adatvédelmi incidens:** a GDPR előírja kötelezettséggként az adatkezelők részére az adatvédelmi incidensek bejelentését. Fontos, hogy az adatfeldolgozóknak ilyen kötelezettsége nincs, kizárólag a saját rendszereit érintő incidenst szükséges jeleznie az adatkezelő felé. Az adatkezelő feladata az általa a tárhelyre telepített programot érintő incidensek észlelése és ha az személyes adatot érint, az adatvédelmi incidens bejelentése, erről nyilvántartás vezetése, szükség esetén az érintett tájékoztatása.

**Ózd, 2018. Március 22.**

  
Dankó István E.V.  
OTP Bank: 11734121-20049320  
Adószám: 66171706-2-25

