

Adatkezelési és -feldolgozási nyilatkozat

a DOCCA Zrt. és a Hunet Kft , a továbbiakban SZOLGÁLTATÓ azon ügyfelei részére, akiknek a SZOLGÁLTATÓ informatikai rendszereket üzemeltet

Verzió: 1.01 Dátum: 2018-05-17

Verzió: 1.02 Dátum: 2018-05-24

Verzió: 1.04 - kimaradt

Verzió: 1.06 Dátum: 2019-01-22 A v1.02 és v1.06 közötti változások aláhúzással jelölve a szövegben.

Verzió: 1.06b mellékletté leválasztás

Verzió: 1.07 Dátum: 2020-09-01 A "Szolgáltató" kifejezés bevezetése.

Verzió: 1.08 Dátum: 2021-04-27 az 1.06-ban bevezetett változási formázások eltávolítása. A releváns helyeket az adatfeldolgozói és adatkezelő szerepkörből adódó eltérések kezelése.

Körülmények: miért születik e nyilatkozat?	1
1. A SZOLGÁLTATÓ nyilatkozata	2
1.1 Milyen személyes adatokat kezel vagy dolgoz fel a SZOLGÁLTATÓ?	2
1.1.1 Ügykezelő rendszer	2
1.1.2 A SZOLGÁLTATÓ megrendelőinek informatikai rendszereiben tárolt adatok elérése	2
1.2. Adatkezelések és adatfeldolgozások módjai, helyzetek	3
1.2.1 Ügyfeleink eszközeinek (és emiatt: adatainak) elérése a munkavégzés során	3
1.2.1.1 Kliens gépek távoli elérése (TeamViewer, VNC, LogMeIn, stb.)	3
1.2.1.2 Szerverek vagy szolgáltatások (G Suite, O365) távoli elérése	3
1.2.1.3 Eszközök fizikai (megrendelőnél helyszíni vagy szervizmunka) elérése	3
1.2.2 Technikai szolgáltatások adattárolással (pl. tárhely, adatmentés, szerverbérlet, spam szűrés)	3
1.2.3 SZOLGÁLTATÓ által igénybevett egyéb szolgáltatók (könyvelő iroda, vírusvédelemi rendszer, külső szerviz, Gmail/G Suite, O365)	3
1.2.4 Ember-ember kommunikáció	4
1.3 Milyen célból kezeli - ha kezeli - a SZOLGÁLTATÓ ezen adatokat?	4
1.4 Mi az adatkezelés jogalapja?	4
1.5 Mi az adatkezelés időtartama?	4
1.6 Milyen biztonsági intézkedéseket tesz a SZOLGÁLTATÓ az adatok védelme érdekében?	5
1.7 Az adatkezelés és adatfeldolgozás helye	5
1.8 Milyen jogokat biztosít a SZOLGÁLTATÓ a személyes adatok kezelésével kapcsolatban?	6
1.9 Mit tesz a SZOLGÁLTATÓ, ha adatvédelmi incidens következik be?	6
1.10 A jogi környezet	6
1.11 A SZOLGÁLTATÓ által igénybevett szolgáltatók avagy Alvállalkozó Adatfeldolgozók	6
2. Külön intézkedés és kérés ügyfeleink felé: GDPR adatok elkülönítése *	7

Körülmények: miért születik e nyilatkozat?

A SZOLGÁLTATÓ és az ügyfelei között informatikai infrastruktúra üzemeltetési szerződések kötettek. Ezen szerződések teljesítése során a SZOLGÁLTATÓ és alvállalkozói (a továbbiakban együttesen értve: SZOLGÁLTATÓ) az ügyfelei informatikai infrastruktúrájához és az ezen tárolt adatokhoz hozzáférnek, hiszen ez a szerződés teljesítéséhez elengedhetetlen. A SZOLGÁLTATÓ ezen helyzet miatt az EU-ban és Magyarországon hatályos adatvédelmi jogszabályokban definiált szerepköröket testesít meg: "adatkezelő" és "adatfeldolgozó" is lehet. Ezen szerepköreiből adódóan adja ki a SZOLGÁLTATÓ ezt a nyilatkozatot.

A SZOLGÁLTATÓ ezen nyilatkozattal rögzít pár tényt ezzel kapcsolatban, emellett e nyilatkozat operatíván az együttműködést érdemben nem érinti.

1. A SZOLGÁLTATÓ nyilatkozata

Török Ákos ügyvezető a SZOLGÁLTATÓ nevében és aláírásra jogosult személyeként az alábbi nyilatkozatot teszem:

1.1 Milyen személyes adatokat kezel vagy dolgoz fel a SZOLGÁLTATÓ?

Ezt a fejezetet az 1.2 részletesebben leírja, azonban azért, hogy ne csökkenjen e nyilatkozat erőssége az előző kiadáshoz képest, megtartottuk ezt a szövegrészt is.

Két fő helyzetről beszélünk:

1.1.1 Ügykezelő rendszer

A SZOLGÁLTATÓ-val való levelezés során a SZOLGÁLTATÓ ügykezelő rendszerében megjelenő adatok. Ezen esetben a SZOLGÁLTATÓ adatkezelő. Ezen helyzetről kijelentjük, hogy a SZOLGÁLTATÓ nem kér és nem gyűjt a GDPR és az Infotörvény szerinti személyes adatot e rendszerbe. Amennyiben valamilyen módon mégis bekerül ide személyes adat, azt a szerződés lezárta után 2 évvel törli a SZOLGÁLTATÓ. Ezen túlmenően üzleti emailcímek, telefonszámok, számítógép felhasználó nevek rendszeresen fordulnak elő a rendszerben, mindezeket a szerződés lezárta után 2 évvel törli a SZOLGÁLTATÓ. Mindezen adatok elkülönítéséről a 2. pontban külön írunk.

1.1.2 A SZOLGÁLTATÓ megrendelőinek informatikai rendszereiben tárolt adatok elérése

- A SZOLGÁLTATÓ mint IT infrastruktúra üzemeltető semmilyen személyes adatot nem gyűjt, információt nem dolgoz fel, továbbá személyek magánszféráját érintő elemzést nem végez az üzemeltetési szolgáltatásai kapcsán, hanem kizárólag a megbízások konkrét céljára irányuló tevékenységet végez: IT infrastruktúrák működőképes állapotát tartja fent és végez ezeken átalakításokat.
- Azonban a SZOLGÁLTATÓ ezen infrastruktúrák üzemeltetése során nagyon sok adathoz hozzáfér, amelyek az infrastruktúrán megtalálhatóak. Ezen adatoknak két fő kategóriája van:

- Technikai adatok, ezeken a SZOLGÁLTATÓ-nak dolgoznia kell. Például: operációs rendszer és szoftverek működését naplózó fájlok, konfigurációs fájlok.
- Felhasználói adatok. Például: adatbázis, e-mail, doc, xls fájlok. Általánosságban és tartalmilag a SZOLGÁLTATÓ nem tudja és nem tud nyilatkozni arról, hogy ezek milyen adatok, hiszen az ügyfelei adatai. Ezek tartalmát öncélúan és konkrét felkérés nélkül a SZOLGÁLTATÓ nem nézi meg, nem vizsgálja, nem elemzi, maga számára öncélúan másolatot nem készít - és ezt a SZOLGÁLTATÓ szigorú belső szabállyal biztosítja 2002. óta. Ezen adatok egyébként lehetnek üzleti és személyes adatok is - azonban a SZOLGÁLTATÓ-nak nincs képessége, kompetenciája és nem is feladata ilyen különbséget tenni, és nem is tesz.

1.2. Adatkezelések és adatfeldolgozások módjai, helyzetek

Csak azon helyzetek tartoznak ide, amikor a megrendelő adatokhoz való hozzáférést ad a SZOLGÁLTATÓ-nak. Ezekből az alábbiakat ismertük eddig fel:

1.2.1 Ügyfeleink eszközeinek (és emiatt: adatainak) elérése a munkavégzés során

Ezen esetek közös jellemzője, hogy az adatokhoz hozzáfér a SZOLGÁLTATÓ, de nem kerül át a SZOLGÁLTATÓ-hoz másolat. Itt a SZOLGÁLTATÓ szabályozása arra irányul, hogy SZOLGÁLTATÓ munkatársai a látott adatokat titokban tartsák. Intézkedések:

- Titoktartási és adatkezelési kötelezettségek vállalása írásban,
- az elérések technikai biztonságának rendszeres felülvizsgálata.

1.2.1.1 Kliens gépek távoli elérése (TeamViewer, VNC, LogMeIn, stb.)

Mikor történik ez? Amikor a SZOLGÁLTATÓ megrendelőjének felhasználója kér valamit (beállítást, hibaelhárítást), ekkor a SZOLGÁLTATÓ kollégái valamilyen távoli elérési megoldással (pl. TeamViewer) érik el a számítógépet.

1.2.1.2 Szerverek vagy szolgáltatások (G Suite, O365) távoli elérése

Mikor történik ez? Példák: amikor kollégáink egy-egy hiba okának keresésekor belépnek a szerverre, és ott dolgoznak - vagy egy új felhasználónak emailcímet hoznak létre.

1.2.1.3 Eszközök fizikai (megrendelőnél helyszíni vagy szervizmunka) elérése

Ez egyszerűen egy számítógép beállítása vagy javítása helyszínen vagy a SZOLGÁLTATÓ irodában.

1.2.2 Technikai szolgáltatások adattárolással (pl. tárhely, adatmentés, szerverbérlet, spam szűrés)

Ezen esetek közös jellemzője, hogy a SZOLGÁLTATÓ infrastruktúráján megtalálhatóak a megrendelők adatai. Itt a SZOLGÁLTATÓ intézkedései:

- A SZOLGÁLTATÓ a rendszerekhez való hozzáférést korlátozza: elérésüket jelszó, VPN és lehetőség szerint multifaktoros autentikáció védi.

1.2.3 SZOLGÁLTATÓ által igénybevett egyéb szolgáltatók (könyvelő iroda, vírusvédelemi rendszer, külső szerviz, Gmail/G Suite, O365)

Ezen esetek közös jellemzője, hogy a megrendelők adatai elvileg harmadik felekhez is átkerülnek. A SZOLGÁLTATÓ intézkedései:

- a SZOLGÁLTATÓ folyamatosan vizsgálja annak lehetőségét, hogy ezen szolgáltatókkal ne osszon meg olyan adatokat, amelyek a GDPR hatálya alá esnek.

1.2.4 Ember-ember kommunikáció

Mikor történik ez? Jellemzően Önöktől valaki és a SZOLGÁLTATÓ-tól valaki egyeztet, pl. egy informatikai kérdés megy a SZOLGÁLTATÓ felé, és annak kapcsán válasz, viszontkérdés. Az adatkezelés az alábbi területeken merül fel a SZOLGÁLTATÓ érdekkörében:

- A kommunikációs közeg:
 - Telefon
 - publikus szakasz (Vodafone, Opennet)
 - SZOLGÁLTATÓ saját telefónia
 - Email és Google Hangout
- A tárolás:
 - A SZOLGÁLTATÓ ügykezelő rendszere (saját rendszer, DOX)
 - Emailek
 - Szerver oldal: Google és Microsoft
 - Kliens eszközök:
 - a SZOLGÁLTATÓ szolgáltatásában résztvevők számítógépei
 - telefonok
 - Fájlok, pl. táblázatok szerkesztése
 - G Suite (G Drive)
 - O365

1.3 Milyen célból kezeli - ha kezeli - a SZOLGÁLTATÓ ezen adatokat?

A SZOLGÁLTATÓ feladata IT infrastruktúra üzemeltetés, aminek a lényege, hogy a megrendelő által meghatározott célra informatikai környezetet biztosítson. Ez például lehet levelező rendszer, fájl (doc, xls) tároló rendszer, weboldalt szolgáltató rendszer. A SZOLGÁLTATÓ elkészíti és/vagy üzemelteti az informatikai környezetet, amelyek ezen adatokat tárolják és az adatokat használó szoftverek működtetését biztosítják, azonban a SZOLGÁLTATÓ magukat az adatokat tartalmilag nem értelmezi. Tehát csupán a munkája során teszi a dolgát ezekkel: a futtatókörnyezet számára elérhetővé és használhatóvá teszi ezen adatokat (pl. számlázó rendszer számára az számla-adatbázist), biztonsági mentést készít ezekről, visszaállít adatokat, stb., és kifejezett kérésre keres szövegrészeket vagy optimalizál adatokat.

1.4 Mi az adatkezelés (és adatfeldolgozás) jogalapja?

Szerződéses kötelezettség.

1.5 Mi az adatkezelés időtartama?

Az ügykezelőből a szerződés lezárását követő 2 év múlva a SZOLGÁLTATÓ törli az adatokat. Az ügyfeleink rendszerein az elérés ad hoc, azaz csak addig érjük el az adatokat, amíg épp be vagyunk jelentkezve az adott rendszerbe, vagy épp biztonsági mentés van nálunk. Ezen adatelérések és -kezelések megszűnnek, amint a SZOLGÁLTATÓ szerződéses kötelezettsége megszűnik.

A SZOLGÁLTATÓ mentési rendszerében a leghosszabb olyan kötelezettségig őrizzük meg az adatokat, amelyek valamilyen törvényi előírás miatt kötelezőek a SZOLGÁLTATÓ-ra nézve. Jelenlegi ismereteink szerint ez NAV vizsgálat kapcsán 8 év. Ezt azonban igyekszünk lerövidíteni a GDPR adatok elkülönítésével*.

1.6 Milyen biztonsági intézkedéseket tesz a SZOLGÁLTATÓ az adatok védelme érdekében?

- A SZOLGÁLTATÓ az ügyfelekkel való kommunikáció során VPN-nel védett ügykezelő rendszert (saját szervereken) és SSL csatornával védett email- és csoportmunka támogató rendszereket (Microsoft O365 és Google Suite rendszereken) használ.
- A SZOLGÁLTATÓ szabályzatban rögzíti és bevált gyakorlata, hogy megrendelői adatairól másolatot csak akkor készít, ha:
 - 1. adatbiztonsági okokból erre szükség van (pl. biztonsági mentés készítése), ehhez azonban minden esetben hozzájárulást kér a megrendelőtől, és a folyamat azon pontján, amikortól sürgősen a biztonsági mentés léte, akkor törli az adatokat;
 - 2. a megrendelő explicit megbízása miatt kell a SZOLGÁLTATÓ-nál másolatnak lennie (pl. adatvisszaállítási feladat, DRP teszt).
- A SZOLGÁLTATÓ ezúton is kifejezetten kéri az ügyfeleit, hogy ne küldjenek GDPR szerinti személyes adatokat a SZOLGÁLTATÓ-nak, mert a SZOLGÁLTATÓ az ügykezelő rendszerből csak extra munkával tud adatokat törölni. A jogszabály vizsgálata és a helyzetünk értékelése alapján a mi céges tevékenységünk során természetesen átadott emailcím és telefonszám nem olyan adatok, amelyek GDPR alá tartoznának.
- A SZOLGÁLTATÓ rendelkezik folyamatokkal és belső szabályozásokkal, amelyek a fenti jogszabályok megfeleléséhez kellene, és folyamatosan bővíti, fejleszti is ezeket.
- ISO27001 bevezetés folyamatban. A dokumentáció releváns részét publikáljuk ügyfeleink részére, amint megfelelő állapotban lesz.
- GDPR adatok elkülönítésével*.

Egyéb megjegyzés a biztonságos adatkezelésről: a SZOLGÁLTATÓ felhívja a figyelmet arra, hogy az email az esetek egy részében nem titkosított kommunikációs csatorna, így a SZOLGÁLTATÓ és az ügyfelei és más levelezőpartnerei közötti úton az emailben küldött adatokat nyilvánosságra hozott adatnak lehet tekinteni, - kivéve, ha titkosított (pl. jelszavas word, zip, pdf, stb.) mellékletben utazik az információ, vagy maga a levél titkosított (S/MIME, PGP, GPG, stb.).

1.7 Az adatkezelés és adatfeldolgozás helye

A SZOLGÁLTATÓ munkatársai gyakran távoli munkavégzést folytatnak az EU országaiban is, és azon kívül is. A SZOLGÁLTATÓ csapatának egy része határon túli magyar, ők többen Kárpátaljáról végzik a munkájukat, így ez eleve elkerülhetetlen a szerződéseink teljesítéséhez. A SZOLGÁLTATÓ minden alvállalkozójával az Európai Bizottság ajánlása szerinti mintaszerződést köti meg az adatkezeléssel kapcsolatban

(<https://eur-lex.europa.eu/legal-content/HU/ALL/?uri=CELEX:32010D0087>)

1.8 Milyen jogokat biztosít a SZOLGÁLTATÓ a személyes adatok kezelésével kapcsolatban?

A SZOLGÁLTATÓ támogatást nyújt ügyfeleinek a GDPR és adatvédelmi jogszabályokban rögzített kötelezettségeik teljesítésében (ideértve az adatkezeléssel kapcsolatos folyamatok vizsgálatára irányuló auditokban való közreműködést is). Ha a fennálló szolgáltatási szerződésben nincs nevesítve a GDPR auditokon való részvétel valamely konkrét szolgáltatásban, akkor SZOLGÁLTATÓ ezt külön díjért teszi, hiszen a szerződés ezt nem fedi le.

1.9 Mit tesz a SZOLGÁLTATÓ, ha adatvédelmi incidens következik be?

1.9.1 Ha a SZOLGÁLTATÓ adatfeldolgozó

Eljár a GDPR 33. cikk 1., 3., 4. és 5. bekezdése, valamint a 34. cikk szerint.

1.9.2 Ha a SZOLGÁLTATÓ adatkezelő

Eljár a GDPR 33. cikk 2. bekezdése szerint.

1.10 A jogi környezet

- A személyes adatok kezelésével kapcsolatosan az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény
- A 2016/679/EU rendelet.
- Azon ügyfeleinknél, ahol egyedi megállapodás is született, és a lentiektől eltérő szabályozást tartalmaz, ott az egyedi megállapodás érvényes.

1.11 A SZOLGÁLTATÓ által igénybevett szolgáltatók avagy Alvállalkozó Adatfeldolgozók

28. cikk (2) *“Az adatfeldolgozó az adatkezelő előzetesen írásban tett eseti vagy általános felhatalmazása nélkül további adatfeldolgozót nem vehet igénybe. Az általános írásbeli felhatalmazás esetén az adatfeldolgozó tájékoztatja az adatkezelőt minden olyan tervezett változásról, amely további adatfeldolgozók igénybevételét vagy azok cseréjét érinti, ezzel biztosítva lehetőséget az adatkezelőnek arra, hogy ezekkel a változtatásokkal szemben kifogást emeljen.”*

Azon ügyfeleinknél, ahol konkrét és a lentiéknél szűkebb lista külön megállapodásban szabályozva van (pl. két konkrét szerveres kolléga dolgozik egy adott infrastruktúrán), ott az adott konkrét, szűkebb megállapodás érvényes.

Az aktuális Alvállalkozó Adatfeldolgozók listája itt található:

https://docs.google.com/document/d/1UeQ56cNI_aGX2VtPsFa-6miul1sYbq9jfaOH4xmJgxw/edit#heading=h.ymf4jl7b9l5p

2. Külön intézkedés és kérés ügyfeleink felé: GDPR adatok elkülönítése *

Ügyfeleink felhívták arra a figyelmet, hogy tágan értelmezve a GDPR-t, minden email, ami nevet, aláírást tartalmaz, az GDPR adatnak minősül. Ezért ha nálunk a legkisebb adatszivárgás történne, egyes GDPR értelmezések szerint ki kellene értesíteni mindenkit, aki emailt küldött nekünk - esetleg ezzel Önöknek, ügyfeleinknek is további teendőt, gondot okozva. Azért, hogy minimalizáljuk az ilyen esetek kihatását, az alábbi fejlesztést készítettük el:

- ha Ön a nekünk küldött email első sorába beírja, hogy: gdpr, akkor a DOX rendszerünk ezeken ügyeket teljesen elkülönített területre helyezi át, amely radikálisan leszűkített hozzáférést enged, és amilyen hamar csak lehetséges, a DOX töröli is ezen adatokat.
- Mikor lehet erre a "gdpr" jelzésre szükség? Mindig, amikor Önök GDPR hatálya alá eső adatot küldenek nekünk. Például: ha Önök új belépő kolléga adatait küldik el nekünk, vagy akár egy hibás excelt vagy Word dokumentumot javításra, amelyben bérlista vagy más személyes adat található.