Docler SSC Kft.
Adatvédelmi és adatbiztonsági Szabályzat

VERZIÓ: 1.0

Hatályos: **2020. február 01.**

Felülvizsgálat határideje: **2021. február 01.**

DOCLER HOLDING

Tartalomjegyzék

A Docler SSC Korlátolt Felelősségű Társaság belső adatkezelési folyamatainak nyilvántartása és az érintettek jogainak biztosítása céljából az alábbi Adatvédelmi és adatbiztonsági Szabályzatot alkotja.

Adatkezelő megnevezése:	Docler SSC Korlátolt Felelősségű Társaság
Adatkezelő cégjegyzékszáma:	01-09-203601
Adatkezelő székhelye:	1101 Budapest, Expo tér 5-7.
Adatkezelő e-elérhetősége:	**csaba.szende@doclerholding.com**

Jelen rendelkezéseket a Docler SSC Korlátolt Felelősségű Társaság többi Szabályzatának előírásaival összhangban kell értelmezni. Amennyiben a személyes adatok védelmével kapcsolatosan ellentmondás áll fent jelen rendelkezések és bármely más, jelen Szabályzat hatálybalépése előtt hatályba lépett Szabályzat előírásai között, úgy abban az esetben jelen rendelkezések az irányadóak.

1. Fogalmak

A jelen Szabályzat alkalmazásában:

- ***Társaság:*** a Szabályzat hatálya alatt adatkezelési tevékenységet végző Docler SSC Korlátolt Felelősségű Társaság.
- ***Szabályzat***: jelen Adatvédelmi és adatbiztonsági szabályzat
- ***GDPR***: a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről szóló, az Európai Parlament és a Tanács (EU) 2016/679 sz. rendelete
- ***személyes adat***: azonosított vagy azonosítható természetes személyre („érintett") vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható;
- ***különleges adat:*** a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a természetes személyek egyedi azonosítását célzó genetikai és biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok;
- ***bűnügyi személyes adat:*** a büntetőeljárás során vagy azt megelőzően a bűncselekménnyel vagy a büntetőeljárással összefüggésben, a büntetőeljárás lefolytatására, illetőleg a bűncselekmények felderítésére jogosult szerveknél, továbbá a büntetés-végrehajtás szervezeténél keletkezett, az érintettel kapcsolatba hozható, valamint a büntetett előéletre vonatkozó személyes adat;
- ***érintett:*** bármely meghatározott, személyes adat alapján azonosított vagy - közvetlenül vagy közvetve - azonosítható természetes személy;
- ***adatkezelő:*** az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely a személyes adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az általa megbízott adatfeldolgozóval végrehajtatja;
- ***adatkezelés:*** a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés;
- ***adatfeldolgozó:*** az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a Társaság nevében személyes adatokat kezel;
- ***címzett***: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, akivel vagy amellyel a személyes adatot közlik, függetlenül attól, hogy harmadik fél-e. Azon

közhatalmi szervek, amelyek egyegyedi vizsgálat keretében az uniós vagy a tagállami joggal összhangban férhetnek hozzá személyes adatokhoz, nem minősülnek címzettnek; az említett adatok e közhatalmi szervek általi kezelése meg kell, hogy feleljen az adatkezelés céljainak megfelelően az alkalmazandó adatvédelmi szabályoknak;

- ***harmadik fél***: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely nem azonos az érintettel, a Társasággal, az adatfeldolgozóval vagy azokkal a személyekkel, akik a Társaság vagy az általa jogszerűen igénybevett adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére felhatalmazást kaptak;
- ***Adatvédelmi Tisztviselő***: a Társaságnál a GDPR 4. szakasza alapján kijelölt és működő adatvédelmi tisztviselő, illetve tisztviselők;
- ***Biztonsági Szolgálat***: a Társaság székhelyének mindenkori vagyonvédelmét ellátó egység. A Biztonsági Szolgálatot a jelen Szabályzat hatályba lépésének napján a Docler Services Kft. (cégjegyzékszám: 01-09-186181; székhely: 1101 Budapest, Expo tér 5-7.) látja el az Irodaház tulajdonosával kötött megállapodás alapján.
- ***hozzájárulás:*** az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez;
- ***adatvédelmi incidens:*** a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi;
- ***NAIH:*** Nemzeti Adatvédelmi és Információszabadság Hatóság; a természetes személyek alapvető jogainak és szabadságainak a személyes adataik kezelése tekintetében történő védelme, valamint a személyes adatok Unión belüli szabad áramlásának megkönnyítése érdekében létrehozott és eljáró, a Társaság adatkezelése fölött felügyeleti jogot gyakorló fő felügyeleti hatóság;
- ***Unió:*** Európai Unió.

2. A Szabályzat célja és hatálya

A Társaság jelen Szabályzat megalkotásával és elérhetővé tételével biztosítani kívánja a GDPR-ban meghatározott alapelveknek megfelelő adatkezelés megvalósulását.

Jelen Szabályzat célja, hogy az érintettek megfelelő tájékoztatást kaphassanak a Társaság által kezelt, illetve az általa megbízott adatfeldolgozó által feldolgozott adatokról, azok forrásáról, az adatkezelés alapelveiről, céljáról, jogalapjáról, időtartamáról, az érintettek jogairól, az adatkezelésbe esetlegesen bevont adatfeldolgozó nevéről, címéről és az adatkezeléssel összefüggő tevékenységéről, továbbá - az érintett személyes adatainak továbbítása esetén - az adattovábbítás jogalapjáról és címzettjéről.

Jelen Szabályzattal a Társaság biztosítani kívánja a nyilvántartások működésének törvényes rendjét, az adatvédelem alkotmányos elveinek, az adatbiztonság követelményeinek érvényesülését, meg kívánja akadályozni az adatokhoz való jogosulatlan hozzáférést, és azok jogosulatlan megváltoztatását, illetve nyilvánosságra hozatalát és szabályozni kívánja a közte és vele egy tulajdonosi körbe tartozó vállalkozások közti adatáramlást és biztosítani az adatvédelmi előírások teljesülését.

A Szabályzat tárgyi hatálya ekként kiterjed a Társaság minden szervezeti egységénél és a jelen Szabályzatot elfogadó és a Társasággal egy tulajdonosi körbe tartozó más vállalkozásnál folytatott valamennyi olyan folyamatra, amely során a GDPR 4. cikk 1. pontjában meghatározott személyes adat kezelése megvalósul.

3. A Társaság által végzett adatkezelés alapelvei

A Társaság személyes adatot csak meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében kezel. A Társaság által kezelt személyes adatok magáncélra való felhasználása tilos. Az adatkezelésnek mindenkor meg kell felelnie a célhoz kötöttség alapelvének.

A Társaság által kezelt személyes adatoknak pontosnak és szükség esetén naprakésznek kell lenniük. A Társaság minden ésszerű intézkedést megtesz annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul töröljék vagy helyesbítsék.

Az adatkezelés során a Társaság minden szükséges intézkedést megtesz az általa végzett személyes adatok jogszerű, tisztességes, valamint az érintett számára átlátható módon történő kezelése érdekében.

A Társaság a személyes adatokat kizárólag az alábbi esetekben kezeli:

a) az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez;
b) az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél, vagy az a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges;
c) az adatkezelés a Társaságra vonatkozó jogi kötelezettség teljesítéséhez szükséges;
d) az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges;
e) az adatkezelés a Társaság vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé, különösen, ha az érintett gyermek.

A Társaság a személyes adatokat a cél eléréséhez megfelelő, releváns és szükséges mértékben kezeli. Az adatkezelési cél megszűnését, illetve az adatkezelési időtartam elteltét követően a Társaság a személyes adatokat végérvényesen törli.

A Társaság az adatkezelés során minden tőle telhetőt megtesz annak érdekében, hogy a megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítsa a személyes adatok biztonságát, beleértve az adatok jogosultalan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is.

4. A belső adatvédelmi rendszer

4.1. Az adatvédelmi rendszer irányítása

A Társaság mindenkori ***vezető tisztségviselője*** a Társaság sajátosságainak figyelembe vételével meghatározza az adatvédelem szervezetét, az adatvédelemre, valamint az azzal összefüggő tevékenységre vonatkozó feladat- és hatásköröket, kijelöli az adatkezelés felügyeletét ellátó személyt.

A Szabályzatban előírtak betartatásáért a feladatkörében minden érintett ***önálló szervezeti egység vezetője*** felelős.

A Társaság ***munkatársai*** munkájuk során gondoskodnak arról, hogy jogosulatlan személyek ne tekinthessenek be személyes adatokba, továbbá arról, hogy a személyes adat tárolása, elhelyezése úgy kerüljön kialakításra, hogy az jogosulatlan személy részére ne legyen hozzáférhető, megismerhető, megváltoztatható, megsemmisíthető.

A Társaság adatvédelmi rendszerének felügyeletét a Társaság vezető tisztségviselője látja el, az általa kinevezett, vagy megbízott adatvédelemért felelős személy(ek), az Adatvédelmi Tisztviselő(k) útján. A Társaság az adatvédelmi feladatok ellátásának elősegítése céljából jogosult Adatvédelmi Bizottság létrehozására. Az Adatvédelmi Bizottság tagjainak megválasztásáról a Társaság legfőbb szerve határoz. Az Adatvédelmi Bizottság létszámát, feladat és hatáskörét, valamint működését a Táraság legfőbb szerve által elfogadott ügyrend határozza meg.

A Társaság vezető tisztségviselője az adatvédelemmel kapcsolatosan:

a) felelős az érintettek GDPR-ban meghatározott jogainak gyakorlásához szükséges feltételek biztosításáért;
b) felelős a Társaság által kezelt személyes adatok védelméhez szükséges személyi, tárgyi és technikai feltételek biztosításáért;
c) felelős az adatkezelésre irányuló ellenőrzés során esetlegesen feltárt hiányosságok, vagy jogszabálysértő körülmények megszüntetéséért, a személyi felelősség megállapításához szükséges eljárás kezdeményezéséért, illetve lefolytatásáért;
d) felügyeli a kinevezett, vagy megbízott belső Adatvédelmi Tisztviselő tevékenységét;
e) vizsgálatot rendelhet el;
f) kiadja a Társaság adatvédelemmel kapcsolatos belső szabályait.

A Társaság ***Adatvédelmi Tisztviselőjének neve, elérhetősége*** *a jelen Szabályzat 1. számú mellékletét* képezi.

Az Adatvédelmi Tisztviselő adatvédelemmel kapcsolatos kötelezettségei:

a) segítséget nyújt az érintett jogainak biztosításában: az érintettek a személyes adatok kezeléséhez és a GDPR szerinti jogaik gyakorlásához kapcsolódó valamennyi kérdésben az Adatvédelmi Tisztviselőhöz fordulhatnak;
b) tájékoztat és szakmai tanácsot ad a Társaság, továbbá az adatkezelést végző alkalmazottak részére a GDPR, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezések szerinti kötelezettségeikkel kapcsolatban;
c) ellenőrzi a GDPR-nak, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezéseknek, továbbá a Társaság vagy az adatfeldolgozó személyes adatok védelmével kapcsolatos belső szabályainak való megfelelést, ideértve a feladatkörök kijelölését, az adatkezelési műveletekben részt vevő személyzet tudatosság-növelését és képzését, valamint a kapcsolódó auditokat is;
d) kérésre szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, valamint nyomon követi a hatásvizsgálat GDPR szerinti elvégzését;
e) minden év január 15-ig jelentést készít a vezető tisztségviselő, vagy ha a Társaságnál ilyen működik, az adatvédelmi bizottság számára a Társaság előző évi adatvédelmi feladatainak végrehajtásáról;
f) jogosult jelen Szabályzat betartását az egyes szervezeti egységeknél ellenőrizni;
g) részt vesz a NAIH által szervezett belső Adatvédelmi Tisztviselők konferenciáján;
h) figyelemmel kíséri az adatvédelemmel és információszabadsággal kapcsolatos jogszabályváltozásokat, ezek alapján, indokolt esetben kezdeményezi jelen Szabályzat módosítását;
i) közreműködik a NAIH-tól a Társasághoz érkezett megkeresések megválaszolásában és a NAIH által kezdeményezett vizsgálat, illetve adatvédelmi hatósági eljárás során;
j) általános állásfoglalás megadása céljából megkeresést fogalmaz meg a NAIH felé, amennyiben egy felmerült adatvédelmi kérdés jogértelmezés útján egyértelműen nem válaszolható meg;
k) együttműködik a NAIH-val; az adatkezeléssel összefüggő ügyekben – ideértve a GDPR szerinti előzetes konzultációt is – kapcsolattartó pontként szolgál a NAIH felé, valamint adott esetben bármely egyéb kérdésben konzultációt folytat vele;

l) időszakosan ellenőrzi a Társaság adatkezeléssel kapcsolatos nyilvántartásait (adatvédelmi incidensek nyilvántartása, adatkezelési tevékenységek nyilvántartása);
m) ha működik a Társaságnál Adatvédelmi Bizottság, részt vesz annak ülésein;
n) ellátja a jelen Szabályzatban feladataként meghatározott egyéb, adatkezeléssel összefüggő feladatokat.

4.2. Adatbiztonsági szabályok

Társaság a jelen Szabályzat szerinti adatkezelés során a jelen Szabályzatban írt intézkedéseket teszi annak érdekében, hogy illetéktelen személyek ne férjenek hozzá a kezelt személyes adatokhoz.

A Társaság munkavállalói a munka törvénykönyvéről szóló 2012. évi I. törvény („Mt.") alapján titoktartásra kötelesek, amely titoktartás őket a munkaviszony megszűnése után is terheli a munkavégzés során megismert személyes adatok tekintetében.

A Társaság a munkavállalóival titoktartási nyilatkozatot ír alá.

A Társaság jogosultsági szinteket dolgoz ki a személyes adatokhoz történő elektronikus és fizikai hozzáférés szabályozására, amelynek technikai részleteit, illetve az informatikai adatbiztonsági előírások részeletes meghatározását az Informatikai Biztonsági Szabályzat tartalmazza.

A Társaság intézkedik annak érdekében, hogy a munkavállalók csak a munkájuk végzéséhez szükséges körben jussanak hozzá a Társaság által kezelt személyes adatokhoz.

A személyes adatok teljes köréhez hozzáférése van a Társaság legfelsőbb vezetőinek, ideértve a vezető tisztségviselőket, illetve az informatikai vezetőt.

Teljeskörű hozzáférés alatt olyan jogosultságot kell érteni, ami lehetővé teszi a személyes adatok módosítását, törlését vagy archiválását is. A hozzáférési szintek kialakítása a Társaság menedzsmentjének a feladata, az operatív kivitelezésről és a kialakított szintek ellenőrzéséről és rendszeres felülvizsgálatáról az Adatvédelmi Tisztviselő gondoskodik.

A papíralapon kezelt személyes adatok biztonsága érdekében a Társaság különösen, de nem kizárólag az alábbi intézkedéseket alkalmazza:

- az adatokat csak az arra jogosultak ismerhetik meg, azokhoz más nem férhet hozzá, más számára fel nem tárhatóak;
- a dokumentumokat jól zárható, száraz, tűzvédelmi és vagyonvédelmi berendezéssel ellátott helyiségben, zárható szekrényben helyezi el;
- a folyamatos, aktív kezelésben lévő iratokhoz csak az illetékesek férhetnek hozzá;
- a dossziék kivételét és visszarakását egy, a szekrényben elhelyezett naplóban szükséges vezetni;
- a Társaság adatkezelést végző munkatársa a nap folyamán csak úgy hagyhatja el az olyan helyiséget, ahol adatkezelés zajlik, hogy a rá bízott adathordozókat elzárja, vagy az irodát bezárja;
- a Társaság adatkezelést végző munkatársa a munkavégzés befejeztével a papíralapú adathordozót elzárja;
- amennyiben a papíralapon kezelt személyes adatok digitalizálásra kerülnek, a digitálisan tárolt dokumentumokra irányadó biztonsági szabályokat alkalmazza a Társaság.

A számítógépen, illetve hálózaton tárolt személyes adatok biztonsága érdekében a Társaság különösen, de nem kizárólag az alábbi intézkedéseket és garanciális elemeket alkalmazza:

- az adatkezelés során használt számítógépek a Társaság tulajdonát képezik, vagy azok fölött tulajdonosi jogkörrel megegyező joggal bír a Társaság;

- a számítógépen található adatokhoz csak érvényes, személyre szóló, azonosítható jogosultsággal – legalább felhasználói névvel és jelszóval – lehet hozzáférni, a jelszavak cseréjéről Társaság rendszeresen gondoskodik;
- az adatokkal történő minden számítógépes rekord nyomon követhetően naplózásra kerül;
- a hálózati kiszolgáló gépen (a továbbiakban: szerver) tárolt adatokhoz csak megfelelő jogosultsággal és csakis az arra kijelölt személyek férhetnek hozzá;
- amennyiben az adatkezelés célja megvalósult, az adatkezelés határideje letelt, úgy az adatot tartalmazó fájl visszaállíthatatlanul törlésre kerül, az adat újra vissza nem nyerhető;
- a hálózaton tárolt adatok biztonsága érdekében a szerveren folyamatos tükrözéssel kerüli el a Társaság az adatvesztést;
- a személyes adatokat tartalmazó adatbázisok aktív adataiból napi mentést végez, a mentés a központi szerver teljes adatállományára vonatkozik és mágneses adathordozóra történik;
- a lementett adatokat tároló mágneses adathordozó az erre a célra kialakított páncéldobozban tűzbiztos helyen és módon tárolt;
- a személyes adatokat kezelő hálózaton a vírusvédelemről folyamatosan gondoskodik;
- a rendelkezésre álló számítástechnikai eszközökkel, azok alkalmazásával megakadályozza illetéktelen személyek hálózati hozzáférését.

A Társaságnál informatikai biztonsági szabályzat van hatályban, mely helyben szokásos módon kihirdetésre került a Társaság minden munkavállalója részére.

5. Az érintettek jogainak érvényesítése

5.1. Tájékoztatás

5.1.1. Tájékoztatás kérelem nélkül

5.1.1.1. Személyes adatok beszerzése az érintettől:

Amennyiben a személyes adatokat a Táraság az érintettől szerezte meg, a Társaság az adatkezelés megkezdése előtt (vagy az érintett hozzájárulásának beszerzését megelőzően) az érintettet egyértelműen, tömör, átlátható érthető és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazva tájékoztatja az alábbiakról:

a) a Társaság, mint adatkezelő neve, illetve elérhetőségei;

b) a személyes adatok tervezett kezelésének célja, valamint az adatkezelés jogalapja;

c) az Adatvédelmi Tisztviselő elérhetőségei;

d) az érintett személyes adatok kategóriái;

e) adott esetben a személyes adatok címzettjei, illetve a címzettek kategóriái, ha van ilyen;

f) adott esetben annak ténye, hogy a Társaság harmadik országba vagy nemzetközi szervezet részére kívánja továbbítani a személyes adatokat, továbbá a Bizottság megfelelőségi határozatának léte vagy annak hiánya, vagy a GDPR 46. cikkben, a 47. cikkben vagy a 49. cikk (1) bekezdésének második albekezdésében említett adattovábbítás esetén a megfelelő és alkalmas garanciák megjelölése, valamint az azok másolatának megszerzésére szolgáló módokra vagy az azok elérhetőségére való hivatkozás;

g) a személyes adatok tárolásának időtartamáról, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjairól;

h) a hozzájáruláson alapuló adatkezelés esetén a hozzájárulás bármely időpontban történő visszavonásához való jog, amely nem érinti a visszavonás előtt a hozzájárulás alapján végrehajtott adatkezelés jogszerűségét;

i) a Társaság vagy egy harmadik fél jogos érdekeinek érvényesítésén alapuló adatkezelés esetén, a Társaság vagy harmadik fél jogos érdekei;

j) az érintett azon jogáról, hogy kérelmezheti a Táraságtól a rá vonatkozó személyes adatokhoz való hozzáférést, azok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen, valamint az érintett adathordozhatósághoz való jogáról;

k) a felügyeleti hatósághoz címzett panasz benyújtásának jogáról;

l) a GDPR 22. cikk (1) és (4) bekezdésében említett automatizált döntéshozatal ténye, ideértve a profilalkotást is, valamint legalább ezekben az esetekben az alkalmazott logikára és arra vonatkozóan érthető információk, hogy az ilyen adatkezelés milyen jelentőséggel, és az érintettre nézve milyen várható következményekkel bír;

m) arról, hogy a személyes adat szolgáltatása jogszabályon vagy szerződéses kötelezettségen alapul vagy szerződés kötésének előfeltétele-e, valamint hogy az érintett köteles-e a személyes adatokat megadni, továbbá hogy milyen lehetséges következményekkel járhat az adatszolgáltatás elmaradása;

A tájékoztatási kötelezettség nem áll fenn, ha és amilyen mértékben az érintett már rendelkezik az adott információkkal.

Amennyiben a Társaság a személyes adatokon a gyűjtésük céljától eltérő célból további adatkezelést kíván végezni, a további adatkezelést megelőzően tájékoztatja az érintettet erről az eltérő célról és a fentiekben említett minden releváns kiegészítő információról.

5.1.1.2. Személyes adatok beszerzése az érintettől eltérő forrásból:

Amennyiben a személyes adatokat a Társaság nem az érintettől szerezte meg, a Társaság egyértelműen, tömör, átlátható érthető és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazva az érintett rendelkezésére bocsátja az alábbi információkat:

a) a fenti 5.1.1. a)-l) pontban foglaltakról;

b) a személyes adatok forrása és adott esetben az, hogy az adatok nyilvánosan hozzáférhető forrásokból származnak-e;

A Társaság a jelen pont szerinti tájékoztatást az alábbiak szerint adja meg:

- a személyes adatok kezelésének konkrét körülményeit tekintetbe véve, a személyes adatok megszerzésétől számított észszerű határidőn, de legkésőbb egy hónapon belül;
- ha a személyes adatokat az érintettel való kapcsolattartás céljára használják, legalább az érintettel való első kapcsolatfelvétel alkalmával; vagy
- ha várhatóan más címzettel is közlik az adatokat, legkésőbb a személyes adatok első alkalommal való közlésekor.

A tájékoztatási kötelezettség nem áll fenn, ha és amilyen mértékben:

a) az érintett már rendelkezik az információkkal;

b) a szóban forgó információk rendelkezésre bocsátása lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényelne, különösen a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból, a GDPR 89. cikk (1) bekezdésében foglalt feltételek és garanciák figyelembevételével végzett adatkezelés esetében, vagy amennyiben e kötelezettség valószínűsíthetően lehetetlenné tenné vagy komolyan veszélyeztetné ezen adatkezelés céljainak elérését. Ilyen esetekben a Társaságnak megfelelő intézkedéseket kell hoznia – az információk nyilvánosan elérhetővé tételét is ideértve – az érintett jogainak, szabadságainak és jogos érdekeinek védelme érdekében;

c) az adat megszerzését vagy közlését kifejezetten előírja a Társaságra alkalmazandó uniós vagy tagállami jog, amely az érintett jogos érdekeinek védelmét szolgáló megfelelő intézkedésekről rendelkezik; vagy

d) a személyes adatoknak valamely uniós vagy tagállami jogban előírt szakmai titoktartási kötelezettség alapján, ideértve a jogszabályon alapuló titoktartási kötelezettséget is, bizalmasnak kell maradnia.

Amennyiben a Társaság a személyes adatokon a gyűjtésük céljától eltérő célból további adatkezelést kíván végezni, a további adatkezelést megelőzően tájékoztatnia kell az érintettet erről az eltérő célról és a fentiekben említett minden releváns kiegészítő információról.

5.1.2. Tájékoztatás az érintett kérelmére

Az érintett kérelmére a Társaság tájékoztatást ad az 5.1.1.1. pont b),d), e), f), g), j), k), l), valamint az 5.1.2.1. b) pontjaiban foglaltak tekintetében.

A Társaság az adatkezelés tárgyát képező személyes adatok másolatát az érintett rendelkezésére bocsátja. Az érintett által kért további másolatokért a Társaság az adminisztratív költségeken alapuló, észszerű mértékű díjat számíthat fel. A másolat igénylésére vonatkozó jog nem érintheti hátrányosan mások jogait és szabadságait.

Ha az érintett elektronikus úton nyújtotta be a kérelmet, az információkat széles körben használt elektronikus formátumban kell rendelkezésre bocsátani, kivéve, ha az érintett másként kéri.

5.2. Helyesbítés

Ha a személyes adat a valóságnak nem felel meg, és a valóságnak megfelelő személyes adat a Társaság rendelkezésére áll, a Társaság az adatot helyesbíti.

Az érintett jogosult arra, hogy kérésére a Társaság indokolatlan késedelem nélkül helyesbítse a rá vonatkozó pontatlan személyes adatokat. Figyelembe véve az adatkezelés célját, az érintett jogosult arra, hogy kérje a hiányos személyes adatok – egyebek mellett kiegészítő nyilatkozat útján történő – kiegészítését.

5.3. Törlés

A Társaság az érintettre vonatkozó személyes adatokat indokolatlan késedelem nélkül törli, ha az alábbi indokok valamelyike fennáll:

a) a személyes adatokra már nincs szükség abból a célból, amelyből azokat gyűjtötték vagy más módon kezelték;

b) az érintett visszavonja az adatkezelés alapját képező hozzájárulását, és az adatkezelésnek nincs más jogalapja;

c) ha az érintett tiltakozása megalapozza a törlést;

d) a személyes adatokat jogellenesen kezelték;

e) a személyes adatokat a Társaságra alkalmazandó uniós vagy tagállami jogban előírt jogi kötelezettség teljesítéséhez törölni kell;

f) a személyes adatok gyűjtésére a GDPR 8. cikk (1) bekezdésében említett, információs társadalommal összefüggő szolgáltatások kínálásával kapcsolatosan került sor.

Amennyiben a Társaság nyilvánosságra hozta a személyes adatot, és azt a fentiek értelmében törölni köteles, az elérhető technológia és a megvalósítás költségeinek figyelembevételével megteszi az észszerűen elvárható lépéseket – ideértve technikai intézkedéseket – annak érdekében, hogy tájékoztassa az adatokat kezelő adatkezelőket, hogy az érintett kérelmezte tőlük a szóban forgó személyes adatokra mutató linkek vagy e személyes adatok másolatának, illetve másodpéldányának törlését.

Az érintett fenti kérelmének teljesítése nem kötelező, amennyiben az adatkezelés:

a) a véleménynyilvánítás szabadságához és a tájékozódáshoz való jog gyakorlása céljából;

b) a személyes adatok kezelését előíró, a Társaságra alkalmazandó uniós vagy tagállami jog szerinti kötelezettség teljesítése céljából;

c) a GDPR 9. cikk (2) bekezdése h) és i) pontjának, valamint a 9. cikk (3) bekezdésének megfelelően a népegészségügy területét érintő közérdek alapján;

d) a GDPR 89. cikk (1) bekezdésével összhangban a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból, amennyiben a kérelem teljesítése valószínűsíthetően lehetetlenné tenné vagy komolyan veszélyeztetné ezt az adatkezelést; vagy

e) jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez

szükséges.

5.4. Az adatkezelés korlátozásához való jog

A Társaság az érintett kérelmére korlátozza az adatkezelést, ha az alábbiak valamelyike teljesül:

a) az érintett vitatja a személyes adatok pontosságát, ez esetben a korlátozás arra az időtartamra vonatkozik, amely lehetővé teszi, hogy a Társaság ellenőrizze a személyes adatok pontosságát;

b) az adatkezelés jogellenes, és az érintett ellenzi az adatok törlését, és ehelyett kéri azok felhasználásának korlátozását;

c) a Társaságnak már nincs szüksége a személyes adatokra adatkezelés céljából, de az érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez; vagy

d) az érintett a GDPR 21. cikk (1) bekezdése szerint tiltakozott az adatkezelés ellen; ez esetben a korlátozás arra az időtartamra vonatkozik, amíg megállapításra nem kerül, hogy a Társaság jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben.

Ha az adatkezelés a fentiek alapján korlátozás alá esik, az ilyen személyes adatokat a tárolás kivételével csak az érintett hozzájárulásával, vagy jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez, vagy más természetes vagy jogi személy jogainak védelme érdekében, vagy az Unió, illetve valamely tagállam fontos közérdekéből lehet kezelni.

A Társaság az érintettet, akinek a kérésére a fentiek alapján korlátozták az adatkezelést, az adatkezelés korlátozásának feloldásáról előzetesen tájékoztatja.

A Társaság minden olyan címzettet tájékoztat a helyesbítésről, törlésről vagy adatkezelés-korlátozásról, akivel, illetve amellyel a személyes adatot közölték, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel. Az érintettet kérésére a Társaság tájékoztatja e címzettekről.

5.5. Adathordozhatósághoz való jog

Az érintett jogosult arra, hogy a rá vonatkozó, általa a Társaság rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja, továbbá jogosult arra, hogy ezeket az adatokat egy másik adatkezelőnek továbbítsa anélkül, hogy ezt akadályozná az a Társaság, amelynek a személyes adatokat a rendelkezésére bocsátotta, ha:

a) az adatkezelés hozzájáruláson, vagy szerződésen alapul; és

b) az adatkezelés automatizált módon történik.

Az érintett jogosult arra, hogy – ha ez technikailag megvalósítható – kérje a személyes adatok adatkezelők közötti közvetlen továbbítását.

A fenti jog gyakorlása nem érintheti hátrányosan mások jogait és szabadságait.

5.6. A tiltakozáshoz való jog

Az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból bármikor tiltakozzon személyes adatainak a GDPR 6. cikk (1) bekezdésének e) (közérdekű adatkezelés) vagy f) pontján (jogos érdek érvényesítésére alapított adatkezelés) alapuló kezelése ellen, ideértve az említett rendelkezéseken alapuló profilalkotást is.

Ebben az esetben a Társaság a személyes adatokat nem kezelheti tovább, kivéve, ha a Társaság bizonyítja, hogy az adatkezelést olyan kényszerítő erejű jogos okok indokolják, amelyek elsőbbséget élveznek az érintett érdekeivel, jogaival és szabadságaival szemben, vagy amelyek jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódnak.

Ha a személyes adatok kezelése közvetlen üzletszerzés érdekében történik, az érintett jogosult arra, hogy bármikor tiltakozzon a rá vonatkozó személyes adatok e célból történő kezelése ellen, ideértve a profilalkotást is, amennyiben az a közvetlen üzletszerzéshez kapcsolódik.

Ha az érintett tiltakozik a személyes adatok közvetlen üzletszerzés érdekében történő kezelése ellen, akkor a személyes adatok a továbbiakban e célból nem kezelhetők.

A Társaság automatizált döntéshozatalt nem alkalmaz, profilalkotást nem végez.

6. Az adatkezeléssel kapcsolatos kérelmének elintézésére vonatkozó szabályok

Ha az érintettektől

- tájékoztatás kérése
- helyesbítés, törlés, illetve korlátozás iránti kérelem
- tiltakozás
- panasz

illetve harmadik személytől adatszolgáltatás iránti, vagy egyéb adatvédelmi tárgyú megkeresés (a továbbiakban jelen pontban együttesen: **„kérelem”**) érkezik a Társasághoz, akkor a megkeresésről tudomást szerző munkavállaló a tudomásszerzést követően haladéktalanul köteles azt továbbítani az Adatvédelmi Tisztviselő számára. A továbbításnak úgy kell megtörténnie, hogy a Társaság az abban foglalt megkeresésnek határidőben eleget tudjon tenni.

Amennyiben a kérelem munkavállalótól, mint érintettől származik, a munkavállaló a kérelmét közvetlenül az Adatvédelmi Tisztviselőnek jogosult eljuttatni.

Az ***Adatvédelmi Tisztviselő*** szükség esetén megkeresi az adatkezelést végző szervezeti egység vezetőjét és a kérelemmel kapcsolatos álláspontját kikéri. Az illetékes a megkeresésre a megkeresés kézhezvételétől számított 5 (öt) munkanapon belül köteles indoklással és intézkedési javaslattal ellátott álláspontját az Adatvédelmi Tisztviselő számára visszajuttatni.

Az Adatvédelmi Tisztviselő a kérelmet és az adatkezelést végző szervezeti egység vezetőjének álláspontját megvizsgálja és ***javaslatot ad a Társaság adatkezelésért felelős, jelen Szabályzat 4. pontjában megjelölt vezetőjének, vagy ha a Társaságnál működik ilyen, az Adatvédelmi Bizottságnak*** a kérelem megválaszolására nyitva álló határidő meghosszabbítása, a kérelem elintézése, illetve indokolt esetben elutasítása tekintetében.

Az információkat írásban vagy más módon – ideértve adott esetben az elektronikus utat is – kell megadni. Az érintett kérésére szóbeli tájékoztatás is adható, feltéve, hogy más módon igazolták az érintett személyazonosságát.

A Társaság vezetője indokolatlan késedelem nélkül, de mindenféleképpen a kérelem beérkezésétől számított ***egy hónapon belül*** tájékoztatja az érintettet a fenti kérelem nyomán hozott intézkedésekről.

Szükség esetén, figyelembe véve a kérelem összetettségét és a kérelmek számát, ez a határidő ***további két hónappal meghosszabbítható***. A határidő meghosszabbításáról a Társaság a késedelem okainak megjelölésével a kérelem kézhezvételétől számított egy hónapon belül tájékoztatja az érintettet.

Ha az érintett elektronikus úton nyújtotta be a kérelmet, a tájékoztatást lehetőség szerint elektronikus úton kell megadni, kivéve, ha az érintett azt másként kéri.

Ha a Társaság vezetője nem tesz intézkedéseket az érintett kérelme nyomán, késedelem nélkül, de legkésőbb a kérelem beérkezésétől számított ***egy hónapon belül*** tájékoztatja az érintettet az intézkedés elmaradásának okairól, valamint arról, hogy az érintett panaszt nyújthat be a NAIH-nál, és élhet bírósági jogorvoslati jogával.

A tájékoztatást ***díjmentesen*** kell biztosítani.

Ha az érintett kérelme egyértelműen megalapozatlan vagy – különösen ismétlődő jellege miatt – túlzó, a Társaság, figyelemmel a kért információ vagy tájékoztatás nyújtásával vagy a kért intézkedés meghozatalával járó ***adminisztratív költségekre***:

- észszerű összegű díjat számíthat fel, vagy
- megtagadhatja a kérelem alapján történő intézkedést.

A kérelem egyértelműen megalapozatlan vagy túlzó jellegének bizonyítása a Társaságot terheli.

Ha a Társaságnak megalapozott kétségei vannak a kérelmet benyújtó természetes személy kilétével kapcsolatban, további, az érintett személyazonosságának megerősítéséhez szükséges információk nyújtását kérheti.

A Társaság kérelmet csak indoklással, írásban utasíthat el.

Az érintett az adatkezeléssel kapcsolatos jogainak gyakorlásával összefüggő bármely kérdésben, különös figyelemmel az adatkezeléssel kapcsolatos jogainak megsértése esetén közvetlenül a Társaság Adatvédelmi Tisztviselőjéhez fordulhat.

Ha az érintett a Társaságnál más személyhez fordul ennek érdekében, az köteles az érintettet tájékoztatni az Adatvédelmi Tisztviselő hatásköréről és elérhetőségeiről.

7. A Társaságnál megvalósuló adatkezelések

7.1. A személyes adatok átadása a Társasággal szerződéses kapcsolatban álló adatkezelőnek, vagy adatfeldolgozónak

A Társaság kizárólag az adatkezelővel vagy adatfeldolgozóval kötött írásbeli megállapodása alapján, az abban foglalt mértékben jogosult az általa kezelt személyes adatok átadására. A Társaság szerződött partnereitől megköveteli a jelen Szabályzatban foglaltak érvényesülését.

7.2. A személyes adatok továbbítása harmadik személyek számára

Az adatkezelést végző munkavállaló bármely adattovábbításra irányuló megkeresés beérkezéséről haladéktalanul tájékoztatja az adatkezelést végző szervezeti egység felelős vezetőjét. Az egység vezetője a rendelkezésre álló adatok alapján megvizsgálja az adattovábbítás feltételeinek fennállását, a kérés teljesíthetőségét, szükség esetén további tájékozódást végez.

Az egység vezetője írásban vagy elektronikus úton tájékoztatja az Adatvédelmi Tisztviselőt. Az adatok továbbításának feltételeinek fennállását az Adatvédelmi Tisztviselő megvizsgálja, és ennek alapján 15 munkanapon belül dönt az adattovábbítás végrehajthatóságáról. Az Adatvédelmi Tisztviselő döntése ellen az adatkérő 8 (nyolc) munkanapon belül panasszal fordulhat a Társaság vezetőjéhez. A Társaság vezetője a panasszal kapcsolatban 15 munkanapon belül hoz döntést.

7.3. Unión kívüli országba vagy nemzetközi szervezetek felé irányuló adattovábbítás

Személyes adatokat az Unión kívüli harmadik országba, vagy nemzetközi szervezetek számára a Társaság kizárólag abban esetben továbbíthat, ha:

a) az Unió Bizottsága határozatával megállapította, hogy a harmadik ország, a harmadik ország valamely területe, vagy egy vagy több meghatározott ágazata, vagy a szóban forgó nemzetközi szervezet megfelelő védelmi szintet biztosít. Az ilyen adattovábbításhoz nem szükséges külön engedély, vagy

b) a harmadik országbeli, vagy nemzetközi szervezetnek minősülő adatkezelő vagy adatfeldolgozó a GDPR 46. cikkében foglalt megfelelő garanciákat nyújtott, és csak azzal a feltétellel, hogy az érintettek számára érvényesíthető jogok és hatékony jogorvoslati lehetőségek állnak rendelkezésre. A garanciáktól függően szükséges, vagy elhagyható az illetékes felügyeleti hatóság engedélye.

A fenti adatszolgáltatással kapcsolatos tényeket, körülményeket dokumentálni kell.

Az Unió Bizottságának megfelelőségi határozata, illetve a GDPR 46. cikk szerinti megfelelő garanciák hiányában – beleértve a kötelező erejű vállalati szabályokat is –, a személyes adatok harmadik ország vagy nemzetközi szervezet részére történő továbbítására vagy többszöri továbbítására csak az alábbi feltételek legalább egyikének teljesülése esetén kerülhet sor:

a) az érintett kifejezetten hozzájárulását adta a tervezett továbbításhoz azt követően, hogy tájékoztatták az adattovábbításból eredő – a megfelelőségi határozat és a megfelelő garanciák hiányából fakadó – esetleges kockázatokról;

b) az adattovábbítás az érintett és a Társaság közötti szerződés teljesítéséhez, vagy az érintett kérésére hozott, szerződést megelőző intézkedések végrehajtásához szükséges;

c) az adattovábbítás a Társaság és valamely más természetes vagy jogi személy közötti, az érintett érdekét szolgáló szerződés megkötéséhez vagy teljesítéséhez szükséges;

d) az adattovábbítás fontos közérdekből szükséges; (a jelen pontban foglalt közérdeket akkor kell figyelembe venni, ha azt az uniós jog vagy a Társaságra vonatkozó tagállami jog elismeri)

e) az adattovábbítás jogi igények előterjesztése, érvényesítése és védelme miatt szükséges;

f) az adattovábbítás az érintett vagy valamely más személy létfontosságú érdekeinek védelme miatt szükséges, és az érintett fizikailag vagy jogilag képtelen a hozzájárulás megadására;

g) a továbbított adatok olyan nyilvántartásból származnak, amely az uniós vagy a tagállami jog értelmében a nyilvánosság tájékoztatását szolgálja, és amely vagy általában a nyilvánosság, vagy az ezzel kapcsolatos jogos érdekét igazoló bármely személy számára betekintés céljából hozzáférhető, de csak ha az uniós vagy tagállami jog által a betekintésre megállapított feltételek az adott különleges esetben teljesülnek. A jelen pont szerinti adattovábbítás nem érintheti a nyilvántartásban szereplő személyes adatok vagy személyes adatok kategóriáinak összességét. Ha a nyilvántartásba kizárólag olyan személyek tekinthetnek be, akiknek ehhez jogos érdeke fűződik, az adattovábbításra kizárólag e személyek kérelmére kerülhet sor, illetve abban az esetben, ha ők a címzettek.

Ha az adattovábbítás nem alapulhat a megfelelőségi határozaton, vagy a GDPR-ban meghatározott garanciákon és a fentiekben említett egyedi helyzetekre vonatkozó eltérések egyike sem alkalmazandó, harmadik országok és nemzetközi szervezetek részére történő adattovábbítás csak akkor történhet, ha az adattovábbítás nem ismétlődő, csak korlátozott számú érintettre vonatkozik, a Társaság olyan kényszerítő erejű jogos érdekében szükséges, amely érdekhez képest nem élveznek elsőbbséget az érintett érdekei, jogai és szabadságai, és a Társaság az adattovábbítás minden körülményét megvizsgálta, és e vizsgálat alapján megfelelő garanciákat nyújtott a személyes adatok védelme tekintetében. A Társaság a vizsgálatot és megfelelő garanciákat az adatkezelési tevékenységek nyilvántartásában dokumentálja.

A Társaságnak tájékoztatnia kell a NAIH-ot az adattovábbításról.

A Társaság a jelen Szabályzat 5.1. pontjában foglalt információk nyújtásán kívül az érintettet tájékoztatja az adattovábbításról, valamint a Társaság kényszerítő erejű jogos érdekéről.

Megfelelőségi határozat hiányában az uniós jog vagy a tagállami jog fontos közérdekből kifejezetten korlátozhatja bizonyos kategóriákba tartozó személyes adatok valamely harmadik országba vagy nemzetközi szervezethez történő továbbítását.

7.4. Ellenőrzés, belső auditok

Az adatvédelemmel kapcsolatos előírások, így különösen a jelen Szabályzat rendelkezéseinek betartását, az adatkezelést végző szervezeti egység vezetői folyamatosan ellenőrizni kötelesek.

Az egyes adatkezelések ellenőrzését szükség szerint, de legalább évente el kell végezni.

Az ellenőrzés tapasztalatairól az Adatvédelmi Tisztviselő írásban tájékoztatja a Társaság vezető tisztségviselőjét, illetve amennyiben a Táraságnál működik, Adatkezelési Bizottságát.

Az Adatvédelmi Tisztviselő tájékoztatása elkészítését megelőzően konzultál az adatkezelésért felelős szervezeti egységek vezetőjével, illetve az illetékes szakemberekkel és javaslatot ad a Társaság vezető tisztségviselőjének/Adatkezelési Bizottságának a szükséges intézkedések megtételére.

Az ellenőrzés során szükségessé vált intézkedések végrehajtásáért a Társaság vezető tisztségviselője felelős.

7.5. Adatvédelmi képzés

A Társaság minden munkavállalója általános adatvédelmi képzésben, illetve évente az ismeretek felfrissítését, további bővítését szolgáló ún. refresh adatvédelmi képzésben köteles részt venni. Az adatvédelmi képzés szervezése, lebonyolítása az Adatvédelmi Tisztviselő feladata.

7.6. Vagyonvédelemmel összefüggő adatkezelések

A Társaság székhelyén kamerás megfigyelőrendszer és beléptető rendszer üzemel, amelynek célja kizárólag a Társaság vagyonának és érdekeinek védelme. A rendszer üzemeltetését a Docler Irodaház mindenkori Biztonsági Szolgálata végzi.

A rendszer üzemeltetésével összefüggésben rögzített adatok tekintetében a Társaság nem végez adatkezelési tevékenységet.

A vagyonvédelemmel kapcsolatos adatkezelés részleteit a Docler Services Kft. kamerás adatkezelésre vonatkozó szabályzata és a Biztonsági Szolgálat vagyonvédelemre vonatkozó szabályzata tartalmazza.

7.7. Adatkezelési tevékenységek nyilvántartása

A Társaság a felelősségébe tartozóan végzett adatkezelési tevékenységekről nyilvántartást vezet. A nyilvántartás a következő információkat tartalmazza:

a) a Társaság neve és elérhetősége, valamint – ha van ilyen – a közös adatkezelőnek, a Társaság képviselőjének és az Adatvédelmi Tisztviselőnek a neve és elérhetősége;

b) az adatkezelés céljai;
c) az érintettek kategóriáinak, valamint a személyes adatok kategóriáinak ismertetése;
d) olyan címzettek kategóriái, akikkel a személyes adatokat közlik vagy közölni fogják, ideértve a harmadik országbeli címzetteket vagy nemzetközi szervezeteket;
e) adott esetben a személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk, beleértve a harmadik ország vagy a nemzetközi szervezet azonosítását, valamint a GDPR 49. cikk (1) bekezdésének második albekezdés szerinti továbbítás esetében a megfelelő garanciák leírása;
f) ahol lehetséges, a különböző adatkategóriák törlésére előirányzott határidők;
g) ahol lehetséges, a GDPR 32. cikk (1) bekezdésében említett technikai és szervezési intézkedések általános leírását.

8. Adatvédelmi incidens kezelése

A Társaságnál felmerülő adatvédelmi incidensek esetén követendő eljárásrendet a Társaság Adatvédelmi Incidenskezelési Szabályzata rögzíti.

9. Új üzleti folyamatok kialakítása során megvalósuló adatkezelés, adatvédelmi hatásvizsgálat

Az új üzleti folyamatok kidolgozása során az üzleti folyamattal érintett szervezeti egység vezetőjének fel szükséges mérnie, hogy az új üzleti folyamat egyben új típusú, eddigi formában nem végzett adatkezelést / adatkezelési folyamatot is jelent-e.

Amennyiben a Társaság által végzett adatkezelés valamely – különösen új technológiákat alkalmazó – típusa –, figyelemmel annak jellegére, hatókörére, körülményére és céljaira, valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, akkor a Társaság az adatkezelést megelőzően hatásvizsgálatot végez arra vonatkozóan, hogy a tervezett adatkezelési műveletek a személyes adatok védelmét hogyan érintik. Olyan egymáshoz hasonló típusú adatkezelési műveletek, amelyek egymáshoz hasonló magas kockázatokat jelentenek, egyetlen hatásvizsgálat keretei között is értékelhetők.

Az adatvédelmi hatásvizsgálat szükségességét az adatkezelésért felelős szervezeti egység vezetője minden egyes új adatkezelés megkezdését megelőzően köteles megvizsgálni és az Adatvédelmi Tisztviselő tanácsát kikérni.

Amennyiben az adatkezelésért felelős szervezeti egység vezetője az adatvédelmi hatásvizsgálatot szükségesnek látja, arról a Társaság vezető tisztségviselője - illetve amennyiben a Társaságnál működik - az Adatvédelmi Bizottság számára előterjesztést készít, amelyhez csatolja az Adatvédelmi Tisztviselő álláspontját is. Amennyiben a Társaságnál működik Adatvédelmi Bizottság, az Adatvédelmi Bizottság az előterjesztést megvizsgálja és javaslatot tesz a Társaság vezető tisztségviselőjének a hatásvizsgálat szükségessége, vagy elhagyhatósága tárgyában.

A hatásvizsgálat végrehajtását az adatkezelést végző szervezeti egység végzi.

Az adatvédelmi hatásvizsgálat elvégzése során az Adatvédelmi Tisztviselő szakmai tanácsát köteles kikérni.

Abban az esetben, amennyiben az új folyamat egyben új adatkezelést is jelent, de adatvédelmi hatásvizsgálatot a Táraság az új adatkezelés tekintetében nem végez, az Adatvédelmi Bizottság, illetve

amennyiben a Társaságnál ilyen nem működik, a Társaság vezető tisztségviselője az Adatvédelmi Tisztviselő véleményének birtokában, az adatkezelésért felelős szervezeti egység vezetője előterjesztése alapján az adatkezelés megfelelősége tekintetében határoz.

10. Jogorvoslat

Az érintett a GDPR, valamint a mindenkori hatályos Polgári Törvénykönyv alapján bíróság előtt érvényesítheti jogait, illetve a NAIH segítségét is kérheti.

A Társaság az érintett adatainak jogellenes kezelésével vagy az adatbiztonság követelményeinek megszegésével másnak okozott kárt, illetve az általa vagy az általa igénybe vett adatfeldolgozó által okozott személyiségi jogsértés esetén járó sérelemdíjat is megtéríti. A Társaság mentesül az okozott kárért való felelősség és a sérelemdíj megfizetésének kötelezettsége alól, ha bizonyítja, hogy a kárt vagy az érintett személyiségi jogának sérelmét az adatkezelés körén kívül eső elháríthatatlan ok idézte elő. Ugyanígy nem téríti meg a kárt, amennyiben az a károsult szándékos vagy súlyosan gondatlan magatartásából származott.

Az érintett a Társaság adatkezelési eljárásával kapcsolatos panasszal a NAIH-hoz fordulhat:

név:	Nemzeti Adatvédelmi és Információszabadság Hatóság
székhely:	1024 Budapest, Szilágyi Erzsébet fasor 22/C.
honlap:	www.naih.hu

11. Hatályba lépés

A jelen Szabályzat a vezető tisztségviselő aláírásával**, 2020. február 01.** napjával lép hatályba.

Kelt: 2020. január 31.

Docler SSC Korlátolt Felelősségű Társaság
Szende Csaba László ügyvezető

Mellékletek

DOCLER HOLDING

1.sz. melléklet

AZ ADATVÉDELMI TISZTVISELŐRE VONATKOZÓ ADATOK

Név:	dr. Koltai Csaba
Telefonszám:	0036-1-432-3000
E-mail cím:	dpo@doclerservices.hu

Az adatkezelés helye:
1101 Budapest, Expo tér 5-7.

Docler SSC Kft.
Data Protection and
Data Security Regulation

VERSION: 1.0

Effective as of:	**February 01, 2020**
Deadline of revision:	**February 01, 2021**

Introduction

Docler SSC Korlátolt Felelősségű Társaság (Docler SSC Limited Liability Company) hereby issues the following Data Protection and Data Security Regulation for the registration of its internal data processing activities and for the protection of the rights of data subjects.

Name of data controller:	Docler SSC Korlátolt Felelősségű Társaság
Company reg. no.:	01-09-203601
Registered office:	1101 Budapest, Expo tér 5-7., Hungary
E-mail:	**csaba.szende@doclerholding.com**

The provisions of the present Regulation shall be interpreted in line with the provisions of the other regulations of Docler SSC Korlátolt Felelősségű Társaság. In the event of any discrepancy related to the protection of personal data between the provisions of the present Regulation and the provisions of any other Regulation that entered into force before the effective date of the present Regulation, then the present Regulation shall prevail.

1. Definitions

Within the application of the present Regulation, the following terms shall have the following meanings:

- ***Company:*** shall mean Docler SSC Korlátolt Felelősségű Társaság that is involved in data controlling activities under the Regulation;
- ***Regulation***: shall mean the present Data Protection and Data Security Regulation;
- ***GDPR***: shall mean regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ;
- ***personal data***: shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
- ***special data:*** shall mean personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation;
- ***personal data processed in criminal matters:*** shall mean personal data that might be related to the data subject or that pertain to any prior criminal offense committed by the data subject and that is obtained by organizations authorized to conduct criminal proceedings or investigations or by penal institutions during or prior to criminal proceedings in connection with a crime or criminal proceedings;
- ***data subject:*** shall mean a natural person who has been identified or is identifiable by reference to any information;
- ***controller:*** shall mean the natural or legal person, or unincorporated body which alone or jointly with others determines the purposes of the processing of data, makes decisions regarding data processing (including the means) and implements such decisions itself or engages a data processor to execute them;
- ***processing:*** shall mean any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
- ***processor:*** shall mean a natural or legal person, public authority, agency or other body which

processes personal data on behalf of the Company;

- ***recipient***: shall mean a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;
- ***third party***: shall mean a natural or legal person, public authority, agency or body other than the data subject, the Company, processor and persons who, under the direct authority of the Company or processor lawfully involved by Company, are authorised to process personal data;
- ***Data Protection Officer***: shall mean the data protection officer or officers appointed by, and operating at, the Company under Section 4 of GDPR;
- ***Security Service***: shall mean the unit that carries out the property protection of the registered office of Company at any given time. On the effective date of the present Regulation, the Security Service is provided by Docler Services Kft. (company registration number: 01-09-186181; registered office: 1101 Budapest, Expo tér 5-7., Hungary) on the basis of an agreement entered into by and between Docler Services Kft. and the owner of the Office Building.
- ***consent:*** shall mean any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;
- ***personal data breach:*** shall mean a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;
- ***NAIH:*** shall mean the Hungarian National Authority for Data Protection and Freedom of Information (Nemzeti Adatvédelmi és Információszabadság Hatóság); i.e. the main supervisory authority established in order to protect the fundamental rights and freedoms of natural persons with regard to the processing of their personal data and to facilitate the free flow of personal data within the Union, which entity acts to supervise the processing activities of the Company;
- ***Union:*** shall mean the European Union.

2. Purpose and Scope of the Regulation

By creating and publishing the present Regulation, Company intends to ensure that its data processing activities are in compliance with the principles laid down in GDPR.

The present Regulation aims to provide data subjects with proper information regarding the data processed by the Company or by the processor involved, the sources thereof, the principles, purpose, grounds, term of processing, the rights of data subjects, the name, address, processing activities of any processor involved, and the grounds and recipients of data forwarding, if any.

With the present Regulation, the Company intends to ensure the lawful operation of the records, the compliance with the constitutional principles of data protection and the requirements of data security, to prevent unauthorized access to, and alteration or disclosure of, the data, and to regulate the data flow between entities owned by the owner(s) of the Company, and ensure compliance with data protection regulations.

Therefore, the scope of the Regulation shall include all processes carried out by any and all organizational units of the Company, and by any and all undertakings agreed to be bound by the present Regulation and owned by the owner(s) of the Company, where the process involves the processing of personal data set out in Article 4 point 1 of GDPR.

3. Principles of Processing by the Company

The Company shall process personal data only for specified purposes, in order to exercise rights or to meet obligations. The data processed by Company shall not be used for private purposes. Processing activities shall, at all times, comply with the purpose limitation principle.

The personal data controlled by Company shall be accurate and, where necessary, kept up to date. Company shall take all reasonable steps to immediately delete or rectify any personal data that is inaccurate for the purposes of data processing.

In the course of data processing, Company shall take all necessary measures to ensure that its processing activities are lawful, fair and transparent for the data subject.

Company shall process personal data only in the following cases:

a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
c) processing is necessary for compliance with a legal obligation to which the Company is subject;
d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
e) processing is necessary for the purposes of the legitimate interests pursued by the Company or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Company processes personal data to the extent proper, relevant and necessary to achieve its purpose. After the termination of the purpose of processing or the expiry term of processing, the Company shall permanently delete the personal data.

In the course of its processing activities, Company shall use its best endeavours in order to ensure appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

4. Internal Data Protection System

4.1. Management of the Data Protection System

The prevailing ***executive officer*** of the Company shall determine the organization of data protection, taking into account the characteristics of the Company, the duties and powers related to data protection and related activities, and shall appoint the person responsible for the supervision of data processing.

The ***manager*** of each relevant ***independent organizational unit*** shall be responsible for ensuring compliance with the Regulation.

In the course of their work, the ***employees*** of Company shall ensure that unauthorized persons cannot access personal data, and that the storage and placement of personal data shall be designed in such a way that they cannot be accessed, known, altered or destroyed by unauthorized persons.

The data protection system of the Company shall be overseen by its executive officer, through the Data Protection Officer(s), the person(s) responsible for data protection, appointed or mandated by the

Company. The Company shall be entitled to establish a Data Protection Committee to facilitate the performance of its data protection tasks. The members of the Data Protection Committee shall be elected by the supreme body of Company. The headcount, functions, powers and operation of the Data Protection Committee shall be governed by rules of procedure adopted by the supreme body of the Company.

In connection with the data protection, the executive officer of Company shall:

a) be responsible for providing the conditions necessary for exercising the rights of data subjects set out in GDPR;
b) be responsible for ensuring the personal, material and technical conditions necessary for the protection of personal data processed by the Company;
c) be responsible for remedying any deficiencies or unlawful circumstances that may have been detected in the course of the data processing audit, and for initiating or conducting the necessary procedures to establish personal liability;
d) oversee the activities of the appointed or mandated Data Protection Officer;
e) be entitled to order an investigation;
f) issue the internal rules and regulations of the Company related to the data protection.

The ***name and contact details of the Data Protection Officer*** *of the Company shall be set out in Schedule 1 of the present Regulation.*

In relation to data protection, the Data Protection Officer shall:

a) provide assistance with data subject rights: data subjects may contact the Data Protection Officer in all matters relating to the processing of their personal data and the exercise of their rights under the GDPR;
b) provide information and professional advice to Company and its employees involved in processing activities regarding their obligations under the GDPR and other EU or Member State data protection provisions;
c) monitor compliance with the GDPR and other EU or Member State data protection provisions, as well as with the internal rules of the Company or its processor on the protection of personal data, including assignment of responsibilities, awareness raising and training of personnel involved in data processing operations; and related audits;
d) provide, upon request, professional advice on the data protection impact assessment and monitor the conduct of the impact assessment under the GDPR;
e) by 15 January each year, report to the executive officer or, where applicable, to the Data Protection Committee, on the performance of the data protection duties of the Company during the preceding year;
f) be entitled to monitor the compliance with the present Regulation at each organizational unit;
g) participate in the conference of Data Protection Officers organized by NAIH;
h) monitor changes in legislation relating to data protection and freedom of information and, where appropriate, initiate amendments to the present Regulation;
i) assist in responding to inquiries from the NAIH to the Company and in the investigation or data protection authority proceedings initiated by NAIH;
j) make a request to the NAIH for a general position where a data protection question cannot be clearly addressed through legal interpretation;
k) cooperate with NAIH; serve as a point of contact for NAIH in relation to data processing issues, including prior consultation under the GDPR, and consult with NAIH in relation to any other question as appropriate;
l) periodically check the records of the Company related to data processing (records of personal data breaches, records of data processing activities);
m) attend the meetings of the Data Protection Committee, if the Company has any;
n) perform any other of its duties related to data processing as set out in the present Regulation.

4.2. Rules of Data Security

The Company shall take the measures described in the present Regulation to prevent unauthorized access to the processed personal data when processing data hereunder.

Pursuant to Act I of 2012 on the Labor Code, the employees of Company shall be bound by a confidentiality obligation, which shall survive the termination of their employment, in respect of the personal data learned in the course of their work.

Company obliges its employees to sign a non-disclosure statement.

Company shall develop authorization levels for the regulation of electronic and physical access to personal data, the technical details of which and the details of the IT data security requirements shall be specified in the IT Security Regulations.

Company shall ensure that employees have access to personal data processed by Company only to the extent necessary for the performance of their work.

The Company's senior executives, including executive officers and IT executive, have access to the full range of personal data.

Full access shall mean access right that allows for the modification, deletion or archiving of personal data. The access levels shall be defined by the management of Company, while the Data Protection Officer shall ensure the operative execution and the recurring audit of the access levels.

In order to ensure the security of the personal data processed as hard copies, Company shall enact, inter alia, the following measures:

- data shall only be accessed by the persons authorized to do so, while data shall not be accessed by, or disclosed to, unauthorized persons;
- documents shall be stored in locked, dry rooms equipped by fire and property protection equipment, in lockable cabinets;
- documents subject to continuous, active processing shall only be accessed by personnel authorized to do so;
- files may be removed from, and placed in, the cabinet by logging the event in a logbook stored in the cabinet;
- the Company's data processing staff may, during the day, leave the premises where the processing takes place only by locking the media or closing the office;
- the Company's data processing staff may, upon the completion/end of the work, lock the hard copy medium;
- in case the personal data stored as hard copy are being digitized, Company shall apply the security rules that pertain to the digitally stored documents.

In order to ensure the security of personal data stored on computers or network, Company shall apply, inter alia, the following measures and safeguards:

- the computers used for the processing activities are owned by Company, or Company has rights over them, which are equivalent to the ownership;
- the data stored on the computer may be accessed only by logging in with a valid, personalized, identifiable account – whereby the login requires the submission of a user name and a password at least –, and Company shall ensure the regular replacement of the passwords;
- all computer records related to the data shall be logged in a way that allows for tracking;
- the data stored on the network server (hereinafter: server) may only be accessed by the designated persons with proper access rights;

- in case the purpose of the processing has been fulfilled and the term of the processing has ended, then the file containing the data shall be deleted irrevocably and therefore data cannot be recovered;
- in order to ensure the data stored in the network, Company shall prevent data loss by creating mirror backups of the data stored on the server on an ongoing basis;
- Company shall create daily backups of the active data of the databases that contain personal data, the backup shall cover all files of the central server and shall be saved on a magnetic medium;
- the magnetic medium that contains the backup shall be stored in the designated safe deposit box at a place, and in a manner, which is fireproof;
- Company shall ensure the continuous protection of the network used for processing personal data against viruses;
- Company shall, with the application of the available IT equipment, prevent the unauthorized access to the network.

There is an IT Security Policy in place at the Company, which has been published to all employees of the Company by means considered customary for the area.

5. Enforcement of Data Subject Rights

5.1. Provision of Information on Processing

5.1.1. Provision of information without being requested

5.1.1.1. Information to be provided where personal data are collected from the data subject:

Where personal data relating to a data subject are collected by Company from the data subject, Company shall, before the commencement of the processing (or before obtaining the consent of the data subject), provide the data subject with all of the following information in a clear, concise, easily accessible form with clear and unambiguous wording:

a) the name and contact details of the Company, as controller;

b) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing ;

c) contact details of the Data Protection Officer;

d) the categories of personal data concerned;

e) the recipients or categories of recipients of the personal data, if any;

f) where applicable, that the Company intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1) of GDPR, reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available;

g) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

h) where the processing is based on the consent of the data subject, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

i) where the processing is based on the legitimate interests pursued by the Company or by a third party, the legitimate interests pursued by the Company or by a third party;

j) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability;

k) the right to lodge a complaint with a supervisory authority;

l) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) of GDPR and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject;

m) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

The obligation of informing the data subject of the above shall not apply where and insofar as the data subject already has the information.

Where the Company intends to further process the personal data for a purpose other than that for which the personal data were obtained, the Company shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to above.

5.1.1.2. Information to be provided where personal data have not been obtained from the data subject:

Where personal data have not been obtained from the data subject, the Company shall provide the data subject with all of the following information in a clear, concise, easily accessible form with clear and unambiguous wording:

a) Information as per Sections 5.1.1. a)-l) above;

b) from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;

The controller shall provide the information referred to above:

- within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed;
- if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or
- if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

The obligation of informing the data subject of the above shall not apply where and insofar as:

a) the data subject already has the information;

b) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) of GDPR or in so far as the above obligation is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the Company shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;

c) obtaining or disclosure is expressly laid down by Union or Member State law to which the Company is subject and which provides appropriate measures to protect the data subject's legitimate interests; or

d) where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.

Where the Company intends to further process the personal data for a purpose other than that for which the personal data were obtained, the Company shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to above.

5.1.2. Provision of information to the request of the data subject

Company shall, upon request, inform the data subject regarding the information set out in Sections 5.1.1.1.

b), d), e), f), g), j), k), l), and Section 5.1.2.1. b).

The Company shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the Company may charge a reasonable fee based on administrative costs. The right to obtain a copy shall not adversely affect the rights and freedoms of others.

Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

5.2. Rectification

In case the personal data proves to be untrue and the Company is in possession of the true personal data, then Company shall rectify the data.

The data subject shall have the right to obtain from the Company without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

5.3. Erasure

Company shall erase personal data concerning the data subject without undue delay where one of the following grounds applies:

a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

b) the data subject withdraws consent on which the processing is based and there is no other legal ground for the processing;

c) the data subject objects to the processing and there are no overriding legitimate grounds for the processing;

d) the personal data have been unlawfully processed;

e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the Company is subject;

f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1) of GDPR.

Where the Company has made the personal data public and is obliged pursuant to the above to erase the personal data, the Company, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

Company is not obliged to comply with data subject requests relating to the above to the extent that processing is necessary:

a) for exercising the right of freedom of expression and information;

b) for compliance with a legal obligation which requires processing by Union or Member State law to which the Company is subject;

c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3) of GDPR;

d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) of GDPR in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

e) for the establishment, exercise or defence of legal claims.

5.4. Right to restriction of processing

The data subject shall have the right to obtain from the Company restriction of processing where one of the following applies:

a) the accuracy of the personal data is contested by the data subject, for a period enabling the Company to verify the accuracy of the personal data;

b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

c) the Company no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims; or

d) the data subject has objected to processing pursuant to Article 21(1) of GDPR pending the verification whether the legitimate grounds of the Company override those of the data subject.

Where processing has been restricted under the above, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

A data subject who has obtained restriction of processing pursuant to the above shall be informed by the Company before the restriction of processing is lifted.

The Company shall communicate any rectification or erasure of personal data or restriction of processing to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The Company shall inform the data subject about those recipients if the data subject requests it.

5.5. Right to data portability

The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to the Company, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the Company to which the personal data have been provided, where:

a) the processing is based on consent or on a contract; and

b) the processing is carried out by automated means.

In exercising his or her right to data portability, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

The exercise of the right to data portability shall not adversely affect the rights and freedoms of others.

5.6. Right to object

The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) (processing based on public interest) or (f) (processing based on legitimate interest) of Article 6(1) of GDPR, including profiling based on those provisions.

The Company shall no longer process the personal data unless the Company demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which

includes profiling to the extent that it is related to such direct marketing.

Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

The Company does not carry out automated decision making or profiling.

6. Rules of processing requests related to data processing

In case the Company receives any request from the data subject for

- information
- rectification, erasure or the restriction of processing
- objection
- complain

or any request submitted by any third party for the provision of data, or any query that is related to data protection (hereinafter collectively: **"request"** for the present chapter), then the employee becoming aware of the request shall forward it to the Data Protection Officer without any delay upon becoming aware of the receipt. The forwarding shall take place in a manner to allow the Company to fulfil the request within the deadline set out therein.

In case the request is originated from an employee, as a data subject, then the employee concerned shall submit the request directly to the Data Protection Officer.

The ***Data Protection Officer*** shall, if necessary, contact the manager of the organizational unit that carries out the processing activity in concern and obtains the opinion of the manager in respect of the request. The manager concerned shall deliver his or her opinion to the Data Protection Officer, together with reasoning and proposals for the actions to be taken, within 5 (five) business days from receiving the request of the Data Protection Officer.

The Data Protection Officer shall inspect the request and the position of the manager of the organizational unit that carries out the processing activity in concern and ***shall provide the executive officer*** **of the Company set out in Section 4 of the present Regulation who is responsible for the processing activity,** ***or the Data Protection Committee, if applicable, with a proposal*** regarding the extension of the deadline for giving reply to the request, or the fulfilment or rejection of the request, where appropriate.

The information shall be given in written form or by other means – including by electronic means, as the case may be. If requested so by the data subject, oral information may also be given, provided that the identity of the data subject has been verified by other means.

The executive officer of the Company shall, without undue delay, but in all cases ***within one month*** from the receipt of the request, inform the data subject of the measures taken on the basis of the above request.

If necessary, considering the complexity of the request and the number of the requests, **this deadline may be extended by two additional months**. Company shall inform the data subject of the extension of the deadline within one month from the receipt of the request; this information shall include the specification of the reason of the delay.

In case the data subject submitted the request by electronic means, the information shall be provided by electronic means, if possible, unless if the data subject requests otherwise.

In case the executive officer of the Company does not take any measures on the basis of the request of the data subject, then the data subject shall be informed thereof without any delay, but not later than ***within one month*** from the receipt of the request of the reasons of not taking measures, and of the right of the data subject to file a complaint with the NAIH or seek judicial remedy.

The information shall be provided ***free of charge***.

Where requests from a data subject are manifestly unfounded or excessive, in particular because of their

repetitive character, the Company may either:

- charge a reasonable fee taking into account the ***administrative costs*** of providing the information or communication or taking the action requested, or
- refuse to act on the request.

The Company shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

When the Company has reasonable doubts concerning the identity of the natural person making the request, the Company may request the provision of additional information necessary to confirm the identity of the data subject.

The Company may refuse any request only in written form and with reasons.

In any matter related to the exercise of the rights of the data subject, with particular attention to the breach of the data subject rights, the data subject may directly contact the Data Protection Officer of the Company.

In case the data subject contacts any other staff member of the Company to this end, the staff member concerned shall inform the data subject of the competences and contact details of the Data Protection Officer.

7. Processing activities of the Company

7.1. Disclosure of the personal data to a controller or processor in contractual relationship with the Company

The Company shall be entitled to disclose personal data processed by Company only on the basis of, and to the extent set out in, the written agreement entered into by and between the Company and the controller or the processor. Company shall require its contractual partners to comply with the provisions of the present Regulations.

7.2. Disclosure of the personal data to third parties

The employee who carries out the processing activity shall, without any delay, inform the responsible manager of the relevant organizational unit of the receipt of any request for disclosure. The manager of the organizational unit shall, on the basis of the data available, assess whether the criteria of disclosure are met, whether the request can be fulfilled, and shall carry out further inquiry, if needed.

The manager of the organizational unit shall inform the Data Protection Officer in written form or by electronic means. The Data Protection Officer shall inspect whether the criteria of disclosure are met, and on the basis thereof, the Data Protection Officer shall, within 15 business days, decide whether the disclosure can be effected or not. The person submitting the request may, within 8 (eight) business days, lodge a complaint to the executive officer of the Company in order to challenge the decision of the Data Protection Officer. The executive officer of the Company shall adopt a decision on the complaint within 15 business days.

7.3. Data transfer to third countries or international organisations

Company may transfer personal data to a third country or an international organisation, provided that:

a) the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorization, or
b) the controller or processor – if seated in a third country or qualifies as an international organization – has provided appropriate safeguards set out in Article 46 of GDPR, and on condition that enforceable data subject rights and effective legal remedies for data subjects are

available. The authorisation from the competent supervisory authority may be required or omitted subject to the safeguards provided.

The facts and circumstances related to the above provision of data shall be documented.

In the absence of the adequacy decision of the Commission of the European Union, or of appropriate safeguards pursuant to Article 46 of GDPR, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:

a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
b) the transfer is necessary for the performance of a contract between the data subject and the Company or the implementation of pre-contractual measures taken at the data subject's request;
c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the Company and another natural or legal person;
d) the transfer is necessary for important reasons of public interest; (public interest referred to in the present point shall be recognised in Union law or in the law of the Member State to which the Company is subject)
e) the transfer is necessary for the establishment, exercise or defence of legal claims;
f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;
g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case. A transfer pursuant to the present point shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. Where the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.

Where a transfer could not be based on an adequacy decision or safeguards set out in GDPR, and none of the derogations for a specific situation referred to above is applicable, a transfer to a third country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the Company which are not overridden by the interests or rights and freedoms of the data subject, and the Company has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The Company shall document the assessment as well as the suitable safeguards in the registry of processing activities.

The Company shall inform NAIH of such transfers.

The Company shall, in addition to providing the information referred to in Section 5.1 of the present Regulation, inform the data subject of the transfer and on the compelling legitimate interests pursued.

In the absence of an adequacy decision, Union or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of personal data to a third country or an international organisation.

7.4. Audit, internal audits

The compliance with the requirements related to data protection, in particular, the compliance with the

provisions of the present Regulation shall be audited on a continuous basis by the managers of the organizational units that carry out processing activities.

The audit of each processing activity shall be carried out as necessary, but on an annual basis at least.

The Data Protection Officer shall inform the executive officer of the Company regarding the conclusions of the audit, or the Data Protection Committee, as the case may be.

Before providing its information, the Data Protection Officer shall consult with the managers of the organizational units responsible for the processing activities, and with the competent professionals, and shall make proposals to the executive officer/Data Protection Committee of the Company regarding the necessary measures to be taken.

The executive officer of the Company shall be responsible for the implementation of the measures became necessary in the course of the audit.

7.5. Data protection trainings

All employees of the Company shall participate in a general data protection training and participate, on an annual basis in so called "refresh" data protection trainings, which serve for the refreshment and further enhancement of the knowledge. The Data Protection Officer shall be responsible for the organization and execution of the trainings.

7.6. Processing activities related to property protection

There is a camera surveillance system and access control system in place at the registered office of the Company, the purpose of which is solely to protect the property and interests of the Company. The system is operated by the prevailing Security Service of the Docler Office Building.

Company does not carry out processing in respect of the data recorded in connection with the operation of the system.

The details of the processing related to property protection are set out in the Camera surveillance-related processing policy of Docler Services Kft. and the property protection policy of the Security Service.

7.7. Records of processing activities

The Company shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:

a) the name and contact details of the Company and, where applicable, the joint controller, the Company's representative and the Data Protection Officer;
b) the purposes of the processing;
c) a description of the categories of data subjects and of the categories of personal data;
d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;
e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1) of GDPR, the documentation of suitable safeguards;
f) where possible, the envisaged time limits for erasure of the different categories of data;
g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1) of GDPR.

8. Handling of privacy breaches

The rules of procedure to be followed in the event of a personal data breach at the Company are set out in the Personal Data Breach Management Policy of the Company.

9. Processing of personal data, data protection impact assessment in the course of creating new business processes

When developing new business processes, the manager of the organizational unit involved in the business process shall assess whether the new business process also involves a new type of data processing activity / data processing process that has not been carried out before in its projected form.

Where a type of processing – carried out by the Company – in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the Company shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

The manager of the organizational unit responsible for the processing shall assess the necessity of the data protection impact assessment before the commencement of each projected processing and seek the advice of the Data Protection Officer.

The manager of the organizational unit responsible for the processing, if deems the data protection impact assessment necessary, shall submit a proposal to the executive officer of the Provider and to the Data Protection Committee, if any, to which the opinion of the Data Protection Officer shall be attached. If there is a Data Protection Committee in place at the Company, it shall inspect the proposal and shall submit a proposal to the executive officer of the Company regarding the necessity or possible omission of the data protection impact assessment.

The data protection impact assessment shall be executed by the organizational unit that carries out the relevant processing activity.

In the course of the execution of the data protection impact assessment, the professional advice of the Data Protection Officer shall be sought.

In case the new process includes a new processing, but the Company does not carry out a data protection impact assessment in respect of the new processing, then the Data Protection Committee, or if there is no such body in place at the Company, the executive officer of the Company shall, after being provided with the opinion of the Data Protection Officer, shall make a decision on the compliance of the processing on the basis of the proposal provided by the manager of the organizational unit responsible for the subject processing.

10. Legal Remedies

Data subjects may enforce their rights before a court of justice on the basis of the GDPR and the prevailing Civil Code of Hungary, or request the assistance of NAIH.

The Company shall compensate the damage caused to others due to the unlawful processing of the data of the data subject or due to the breach of the data security requirements, or the grievance fee payable for the infringement of moral rights caused by the Company or by any processor involved by the Company.

The Company shall not be liable for the damage caused, and for the payment of the grievance fee, if the Company evidences that the damage or the infringement of the moral rights of the data subject has been caused by an unavoidable reason not attributable to the processing. Identically, the Company shall not compensate any damage caused by the intentional or grossly negligent conduct of the injured party.

The data subject may contact NAIH with complaints related to any processing activity of the Company:
name: Nemzeti Adatvédelmi és Információszabadság Hatóság
registered office: 1024 Budapest, Szilágyi Erzsébet fasor 22/C.
website: www.naih.hu

11. Effective Date

The present Policy shall enter into force, upon signature by the executive officer**, on February 01, 2020**.

Date: January 31, 2020

Docler SSC Korlátolt Felelősségű Társaság
Szende Csaba László Managing Director

Schedules

Schedule No. 1

NAME AND CONTACT DETAILS OF THE DATA PROTECTION OFFICER

Name:	dr. Koltai Csaba
Telephone:	0036-1-432-3000
E-mail:	dpo@doclerservices.hu

Venue of processing activities:
1101 Budapest, Expo tér 5-7.