ADATVÉDELMI SZABÁLYZAT

Tartalom

Bevezető..... 2
1. A szabályzat célja és hatálya..... 2
2. Fogalmak..... 3
3. Az adatkezelések szabályai..... 5
4. A Társaság adatvédelmi rendszere..... 9
5. Adatvédelmi incidens kezelése..... 11
Adatvédelmi incidens észlelése és jelentése..... 11
Adatvédelmi incidens kivizsgálása, értékelése..... 11
Az adatvédelmi incidens nyilvántartása..... 12
Az adatvédelmi incidens bejelentése a Hatóság részére..... 12
Az érintettek tájékoztatása az adatvédelmi incidensről..... 12
6. Adatbiztonsági szabályok..... 13
Fizikai védelem..... 13
Informatikai védelem..... 13
Jogosultságkezelés..... 14
7. Álnevesítés..... 14
8. Beépített adatvédelem..... 15
9. Az érintettek jogainak érvényesítése..... 16
10. Az adatkezelő és adatfeldolgozók köre..... 17
Az adatkezelő..... 17
Adatfeldolgozók..... 18
11. Az adatkezelés jogalapja..... 18
12. A felhasználó jogai..... 19

Bevezető

Süli Richárd EV. (a továbbiakban: Adatkezelő) belső adatkezelési folyamatainak nyilvántartása és az érintettek jogainak biztosítása céljából az alábbi Adatvédelmi és adatbiztonsági szabályzatot (a továbbiakban: szabályzat) alkotja.

Adatkezelő megnevezése: Süli Richárd EV.
Adatkezelő rövidített elnevezés: -
Adatkezelő adószáma: 66530642-1-33
Adatkezelő székhelye: 2241 Sülysáp Széchenyi utca 18.
Adatkezelő e-elérhetősége: suli.richard@gmail.Com
Adatkezelő képviselője: Süli Richárd

Jelen rendelkezéseket a Társaság többi szabályzatának előírásaival összhangban kell értelmezni. Amennyiben a személyes adatok védelmével kapcsolatosan ellentmondás áll fent jelen rendelkezések és a bármely más, jelen szabályzat hatálybalépése előtt hatályba lépett szabályzat előírásai között, úgy abban az esetben jelen rendelkezések az irányadóak. Jelen szabályzatban használt rövidítések az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény a munka törvénykönyvéről szóló 2012. évi I. törvény a munkavédelemről szóló 1993. évi XCIII. törvény a polgári törvénykönyvről szóló 2013. évi V. törvény a számvitelről szóló 2000. évi C. törvény a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól szóló 2005. évi CXXXIII. törvény az Európai Parlament és a Tanács (EU) 2016/679 rendelete az Európai Parlament és a Tanács (EU) 2016/679 rendelete Infotv. Mt. Mvt. Ptk. Sztv. Szvtv. GDPR vagy Rendelet NAIH vagy Hatóság

1. A szabályzat célja és hatálya A Társaság jelen szabályzat megalkotásával és elérhetővé tételével biztosítani kívánja az Infotv. 15. §- ában meghatározott érintetti tájékoztatáshoz való jog megvalósulását. A szabályzat célja, hogy az érintettek megfelelő tájékoztatást kaphassanak a Társaság által kezelt, illetve az általa megbízott adatfeldolgozó által feldolgozott adatokról, azok forrásáról, az adatkezelés céljáról, jogalapjáról, időtartamáról, az adatkezelésbe esetlegesen bevont adatfeldolgozó nevéről, címéről és az adatkezeléssel összefüggő tevékenységéről, továbbá - az érintett személyes adatainak továbbítása esetén - az adattovábbítás jogalapjáról és címzettjéről. A 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. A szabályzat tárgyi hatálya kiterjed a Társaság minden szervezeti egységénél folytatott valamennyi olyan folyamatra, amely során az Infotv. 3. § 2. pontjában meghatározott személyes adat kezelése megvalósul. A szabályzat időbeli hatálya 2018.02.01-jétől visszavonásig tart.

2. Fogalmak A jelen szabályzat fogalmi rendszere megegyezik az Infotv.-ben és a GDPR-ban meghatározott értelmező fogalommagyarázatokkal, így különösen: Érintett Személyes adat Különleges adat Bűnügyi személyes adat Hozzájárulás Tiltakozás Adatkezelő Adatkezelés Adattovábbítás Nyilvánosságra hozatal Adattörlés Adatzárolás Adatmegjelölés Adatmegsemmisítés Adatfeldolgozás Adatfeldolgozó Adatállomány Harmadik személy EGT-állam Harmadik ország Adatvédelmi incidens Adatkezelés bármely meghatározott, személyes adat alapján azonosított vagy - közvetlenül vagy közvetve - azonosítható természetes személy; az érintettel kapcsolatba hozható adat - különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret -, valamint az adatból levonható, az érintettre vonatkozó következtetés; a faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviseleti szervezeti

tagságra, a szexuális életre vonatkozó személyes adat, az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat, valamint a bűnügyi személyes adat; a büntetőeljárás során vagy azt megelőzően a bűncselekménnyel vagy a büntetőeljárással összefüggésben, a büntetőeljárás lefolytatására, illetve a bűncselekmények felderítésére jogosult szerveknél, továbbá a büntetés-végrehajtás szervezeténél keletkezett, az érintettel kapcsolatba hozható, valamint a büntetett előéletre vonatkozó személyes adat; az érintett akaratának önkéntes és határozott kinyilvánítása, amely megfelelő tájékoztatáson alapul, és amellyel félreérthetetlen beleegyezését adja a rá vonatkozó személyes adat - teljes körű vagy egyes műveletekre kiterjedő - kezeléséhez; az érintett nyilatkozata, amellyel személyes adatának kezelését kifogásolja, és az adatkezelés megszüntetését, illetve a kezelt adat törlését kéri; az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely önállóan vagy másokkal együtt az adat kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja; az alkalmazott eljárástól függetlenül az adaton végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adat további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS- minta, íriszkép) rögzítése; az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele; az adat bárki számára történő hozzáférhetővé tétele; az adat felismerhetetlenné tétele oly módon, hogy a helyreállítása többé nem lehetséges; az adat azonosító jelzéssel ellátása további kezelésének végleges vagy meghatározott időre történő korlátozása céljából; az adat azonosító jelzéssel ellátása annak megkülönböztetése céljából; az adatot tartalmazó adathordozó teljes fizikai megsemmisítése; az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől, feltéve, hogy a technikai feladatot az adaton végzik; az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely szerződés alapján - beleértve a jogszabály rendelkezése alapján kötött szerződést is - adatok feldolgozását végzi; az egy nyilvántartásban kezelt adatok összessége; olyan természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely nem azonos az érintettel, az adatkezelővel vagy az adatfeldolgozóval; az Európai Unió tagállama és az Európai Gazdasági Térségről szóló megállapodásban részes más állam, továbbá az az állam, amelynek állampolgára az Európai Unió és tagállamai, valamint az Európai Gazdasági Térségről szóló megállapodásban nem részes állam között létrejött nemzetközi szerződés alapján az Európai Gazdasági Térségről szóló megállapodásban részes állam állampolgárával azonos jogállást élvez; minden olyan állam, amely nem EGT-állam; személyes adat jogellenes kezelése vagy feldolgozása, így különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés; a tárolt személyes adatok megjelölése jövőbeli kezelésük korlátozása céljából; korlátozása Álnevesítés Biometrikus adat Címzett Egészségügyi adat Harmadik fél Genetikai adat Képviselő Kötelező erejű vállalati szabályok Nyilvántartási rendszer Profilalkotás Releváns és megalapozott kifogás Tevékenységi központ a személyes adatok olyan módon történő kezelése, amelynek következtében további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik, feltéve, hogy az ilyen további információt külön tárolják, és technikai és szervezési intézkedések megtételével biztosított, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet kapcsolni; egy természetes személy testi, fiziológiai vagy viselkedési jellemzőire vonatkozó minden olyan sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását, ilyen például az arckép vagy a daktiloszkópiai adat; 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 egy egyedi 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; egy természetes személy testi vagy pszichikai egészségi állapotára vonatkozó személyes adat, ideértve a természetes személy számára nyújtott egészségügyi szolgáltatásokra vonatkozó olyan adatot is, amely információt hordoz a

természetes személy egészségi állapotáról; az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely nem azonos az érintettel, az adatkezelővel, az adatfeldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére felhatalmazást kaptak; egy természetes személy örökölt vagy szerzett genetikai jellemzőire vonatkozó minden olyan személyes adat, amely az adott személy fiziológiájára vagy egészségi állapotára vonatkozó egyedi információt hordoz, és amely elsősorban az említett természetes személyből vett biológiai minta elemzéséből ered; az az Unióban tevékenységi hellyel, illetve lakóhellyel rendelkező és az adatkezelő vagy adatfeldolgozó által írásban megjelölt természetes vagy jogi személy, aki, illetve amely az adatkezelőt vagy adatfeldolgozót képviseli az adatkezelőre vagy adatfeldolgozóra az e rendelet értelmében háruló kötelezettségek vonatkozásában; a személyes adatok védelmére vonatkozó szabályzat, amelyet az Unió valamely tagállamának területén tevékenységi hellyel rendelkező adatkezelő vagy adatfeldolgozó egy vagy több harmadik országban a személyes adatoknak az ugyanazon vállalkozáscsoporton vagy közös gazdasági tevékenységet folytató vállalkozások ugyanazon csoportján belüli adatkezelő vagy adatfeldolgozó részéről történő továbbítása vagy ilyen továbbítások sorozata tekintetében követ; a személyes adatok bármely módon – centralizált, decentralizált vagy funkcionális vagy földrajzi szempontok szerint – tagolt állománya, amely meghatározott ismérvek alapján hozzáférhető; személyes adatok automatizált kezelésének bármely olyan formája, amelynek során a személyes adatokat valamely természetes személyhez fűződő bizonyos személyes jellemzők értékelésére, különösen a munkahelyi teljesítményhez, gazdasági helyzethez, egészségi állapothoz, személyes preferenciákhoz, érdeklődéshez, megbízhatósághoz, viselkedéshez, tartózkodási helyhez vagy mozgáshoz kapcsolódó jellemzők elemzésére vagy előrejelzésére használják; a döntéstervezettel szemben benyújtott, azzal kapcsolatos kifogás, hogy ezt a rendeletet megsértették-e, illetve, hogy az adatkezelőre vagy az adatfeldolgozóra vonatkozó tervezett intézkedés összhangban van-e a rendelettel; a kifogásban egyértelműen be kell mutatni a döntéstervezet által az érintettek alapvető jogaira és szabadságaira, valamint adott esetben a személyes adatok Unión belüli szabad áramlására jelentett kockázatok jelentőségét; az egynél több tagállamban tevékenységi hellyel rendelkező adatkezelő esetében az Unión belüli központi ügyvitelének helye, ha azonban a személyes adatok kezelésének céljaira és eszközeire vonatkozó döntéseket az adatkezelő egy Unión belüli másik tevékenységi helyén hozzák, és az utóbbi tevékenységi hely rendelkezik hatáskörrel az említett döntések végrehajtatására, az említett döntéseket meghozó tevékenységi helyet kell tevékenységi központnak tekinteni; az egynél több tagállamban tevékenységi hellyel rendelkező adatfeldolgozó esetében az Unión belüli központi ügyvitelének helye, vagy ha az adatfeldolgozó az Unióban nem rendelkezik központi ügyviteli hellyel, akkor az adatfeldolgozónak az az Unión belüli tevékenységi helye, ahol az adatfeldolgozó tevékenységi helyén folytatott tevékenységekkel összefüggésben végzett fő adatkezelési tevékenységek zajlanak, amennyiben az adatfeldolgozóra e rendelet szerint meghatározott kötelezettségek vonatkoznak; Vállalkozás Vállalkozáscsoport gazdasági tevékenységet folytató természetes vagy jogi személy, függetlenül a jogi formájától, ideértve a rendszeres gazdasági tevékenységet folytató személyegyesítő Társaságokat és egyesületeket is; az ellenőrző vállalkozás és az általa ellenőrzött vállalkozások. Amennyiben a mindenkori hatályos adatvédelmi jogszabály (jelen szabályzat megalkotásakor az Infotv. és a GDPR) fogalommagyarázatai eltérnek jelen szabályzat fogalommagyarázataitól, akkor a jogszabály által meghatározott fogalmak az irányadók.

3. Az adatkezelések szabályai Mivel az információs önrendelkezés minden természetes személy Alaptörvényben rögzített alapjoga, így a Társaság eljárásai során csak és kizárólag a hatályos jogszabályok rendelkezései alapján végez adatkezelést. Személyes adat kezelésére csak jog gyakorlása vagy kötelezettség teljesítése érdekében van lehetőség. A Társaság által kezelt személyes adatok magáncélra való felhasználása tilos. Az adatkezelésnek mindenkor meg kell felelnie a célhoz kötöttség alapelvének. A Társaság személyes adatot csak meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében kezel, a cél eléréséhez szükséges minimális mértékben és ideig. Az adatkezelés minden szakaszában meg kell felelnie a célnak – és amennyiben az adatkezelés célja megszűnt, vagy az adatok kezelése egyébként jogellenes, az adatok törlésre kerülnek. A törlésről a Társaságnak az adatot ténylegesen kezelő munkavállalója gondoskodik. A törlést a munkavállaló felett munkáltatói jogköröket ténylegesen gyakorló személy ellenőrizheti. A Társaság személyes adatot csak az érintett előzetes – különleges személyes adat esetén írásbeli – hozzájárulása vagy törvény, illetve törvényi

felhatalmazás alapján kezel. A Társaság az adat felvétele előtt minden esetben közli az érintettel az adatkezelés célját, valamint az adatkezelés jogalapját. A Társaság szervezeti egységeinél adatkezelést végző alkalmazottak és a Társaság megbízásából az adatkezelésben résztvevő, annak valamely műveletét végző szervezetek alkalmazottjai kötelesek a megismert személyes adatokat üzleti titokként megőrizni. A személyes adatokat kezelő és azokhoz hozzáférési lehetőséggel rendelkező személyek kötelesek Titoktartási nyilatkozatot tenni. Ha a szabályzat hatálya alatt álló személy tudomást szerez arról, hogy a Társaság által kezelt személyes adat hibás, hiányos vagy időszerűtlen, köteles azt helyesbíteni vagy helyesbítését az adat rögzítéséért felelős munkatársnál kezdeményezni. A Társaság megbízásából adatfeldolgozói tevékenységet végző természetes vagy jogi személyekre, illetve jogi személyiséggel nem rendelkező szervezetekre vonatkozó adatvédelmi kötelezettségeket az adatfeldolgozóval kötött megbízási szerződésben érvényesítendők. Az adatfeldolgozóval a Társaság az Infotv. által előírt Adatfeldolgozói szerződést köt (15. sz. melléklet).

3.1 Munkaügyi, személyzeti nyilvántartás A munkavállalóktól kizárólag olyan adatok kérhetők és tarthatók nyilván, valamint olyan munkaköri orvosi alkalmassági vizsgálatok végezhetők, amelyek munkaviszony létesítéséhez, fenntartásához és megszüntetéséhez, illetve a szociális-jóléti juttatások biztosításához szükségesek és a munkavállaló személyhez fűződő jogait nem sértik. A Társaság munkáltatói jogos érdekeinek érvényesítése (Rendelet 6. cikk (1) bekezdése f)) jogcímén munkaviszony létesítése, teljesítése vagy megszűnése céljából kezeli a munkavállaló alábbi adatait: 1. név 2. születési név 3. születési ideje 4. anyja neve 5. lakcíme 6. állampolgársága 7. adóazonosító jele 8. TAJ száma 9. nyugdíjas törzsszám (nyugdíjas munkavállaló esetén) 10. telefonszám 11. e-mail cím 12. személyi igazolvány száma 13. lakcímet igazoló hatósági igazolvány száma 14. bankszámlaszáma 15. online azonosító (ha van) 16. munkába lépésének kezdő és befejező időpontja, 17. munkakör 18. iskolai végzettségét, szakképzettségét igazoló okmány másolata 19. fénykép 20. önéletrajz 21. munkabérének összege, a bérfizetéssel, egyéb juttatásaival kapcsolatos adatok, 22. a munkavállaló munkabéréből jogerős határozat vagy jogszabály, illetve írásbeli hozzájárulása alapján levonandó tartozást, illetve ennek jogosultságát 23. a munkavállaló munkájának értékelése 24. a munkaviszony megszűnésének módja, indokai 25. munkakörtől függően erkölcsi bizonyítványa 26. a munkaköri alkalmassági vizsgálatok összegzése 27. magánnyugdíjpénztári és önkéntes kölcsönös biztosító pénztári tagság esetén a pénztár megnevezése, azonosító száma és a munkavállaló tagsági száma 28. külföldi munkavállaló esetén útlevélszám; munkavállalási jogosultságot igazoló dokumentumának megnevezését és száma 29 munkavállalót ért balesetek jegyzőkönyveiben rögzített adatokat 30. a jóléti szolgáltatás, kereskedelmi szálláshely igénybe vételéhez szükséges adatokat 31. a Társaságnál biztonsági és vagyonvédelmi célból alkalmazott kamera és beléptető rendszer,illetve a helymeghatározó rendszerek által rögzített adatokat. Betegségre és szakszervezeti tagságára vonatkozó adatokat a munkáltató csak a Munka Törvénykönyvben meghatározott jog, vagy kötelezettség teljesítése céljából kezel. A személyes adatok címzettjei: a munkáltató vezetője, munkáltatói jogkör gyakorlója, a Társaság munkaügyi feladatokat ellátó munkavállalói és adatfeldolgozói. A személyes adatok tárolásának időtartama: a munkaviszony megszűnését követő 3 év, valamint a szolgálati jogosultság megállapításához, nyugdíjellátás megállapításához szükséges adatok vonatkozásában 50 év. Az érintett munkavállalóval az adatkezelés megkezdése előtt közölni kell, hogy az adatkezelés a Munka törvénykönyvén és a munkáltató jogos érdekeinek érvényesítésén alapul

3.2 Alkalmassági vizsgálatokkal kapcsolatos adatkezelés A munkavállalóval szemben csak olyan alkalmassági vizsgálat alkalmazható, amelyet munkaviszonyra vonatkozó szabály ír elő, vagy amely munkaviszonyra vonatkozó szabályban meghatározott jog gyakorlása, kötelezettség teljesítése érdekében szükséges. A vizsgálat előtt részletesen tájékoztatni kell a munkavállalókat többek között arról, hogy az alkalmassági vizsgálat milyen készség, képesség felmérésére irányul, a vizsgálat milyen eszközzel, módszerrel történik. Amennyiben jogszabály írja elő a vizsgálat elvégzését, akkor tájékoztatni kell a munkavállalókat a jogszabály címéről és a pontos jogszabályhelyről is. A munkaalkalmasságra, felkészültségre irányuló tesztlapok a munkáltató mind a munkaviszony létesítése előtt, mind pedig a munkaviszony fennállása alatt kitöltetheti a munkavállalókkal. Az egyértelműen munkaviszonnyal kapcsolatos, a munkafolyamatok hatékonyabb ellátása, megszervezése érdekében csak akkor tölthető ki a munkavállalók nagyobb csoportjával pszichológiai, vagy személyiségjegyek kutatására alkalmas tesztlap, ha az elemzés során felszínre került adatok nem köthetők az egyes

konkrét munkavállalókhoz, vagyis anonim módon történik az adatok feldolgozása. A kezelhető személyes adatok köre: a munkaköri alkalmasság ténye, és az ehhez szükséges feltételek. Az adatkezelés jogalapja: a munkáltató jogos érdeke. A személyes adatok kezelésének célja: munkaviszony létesítése, fenntartása, munkakör betöltése. A személyes adatok címzettjei, illetve a címzettek kategóriái: A vizsgálat eredményt a vizsgált munkavállalók, illetve a vizsgálatot végző szakember ismerhetik meg. A munkáltató csak azt az információt kaphatja meg, hogy a vizsgált személy a munkára alkalmas-e vagy sem, illetve milyen feltételek biztosítandók ehhez. A vizsgálat részleteit, illetve annak teljes dokumentációját azonban a munkáltató nem ismerheti meg. A személyes adatok kezelésének időtartama: a munkaviszony megszűnését követő 3 év.

3.3 Felvételre jelentkező munkavállalók adatainak kezelése, pályázatok, önéletrajzok A kezelhető személyes adatok köre: a természetes személy neve, születési ideje, helye, anyja neve, lakcím, képesítési adatok, fénykép, telefonszám, e-mail cím, a jelentkezőről készített munkáltatói feljegyzés (ha van). A személyes adatok kezelésének célja: jelentkezés, pályázat elbírálása, a kiválasztott pályázóval munkaszerződés kötése. Az érintettet tájékoztatni kell arról, ha a munkáltató nem őt választotta az adott állásra. Az adatkezelés jogalapja: az érintett hozzájárulása. A személyes adatok címzettjei, illetve a címzettek kategóriái: a Társaságnál munkáltatói jogok gyakorlására jogosult vezető, munkaügyi feladatokat ellátó munkavállalók. A személyes adatok tárolásának időtartama: A jelentkezés, pályázat elbírálásáig. A ki nem választott jelentkezők személyes adatait törölni kell. Törölni kell annak adatait is, aki jelentkezését, pályázatát visszavonta. A munkáltató csak az érintett kifejezett, egyértelmű és önkéntes hozzájárulása alapján őrizheti meg a pályázatokat, feltéve, ha azok megőrzésére a jogszabályokkal összhangban álló adatkezelési célja elérése érdekében szükség van. E hozzájárulást a felvételi eljárás lezárását követően kell kérni a jelentkezőktől.

3.4 A Társaság által működtetett Úszóiskola tanulóinak és törvényes képviselőik adatainak kezelése A kezelhető személyes adatok köre: a természetes személy neve, születési ideje, helye, anyja neve, lakcím, úszástudás szintje, egészségügyi megfelelés (nincs fertőződ betegsége, ami a közösségi létesítmény igénybevételének akadályát képezné) fénykép, telefonszám, e-mail cím. Amennyiben az Úszóiskola tanulója kiskorú, úgy a személyes adatok kezeléséhez a törvényes képviselő (szülő, gyám) hozzájárulása szükséges. Ebben az esetben a törvényes képviselőre vonatkozóan kezelhető személyes adatok köre a következő: a természetes személy neve, anyja neve, lakcím, telefonszám, e-mail cím. Az adatkezelés célja: a tanuló adatai vonatkozásában az úszásoktatás megvalósítása, a törvényes képviselő adatai vonatkozásában: kiskorú gyermek törvényes képviselőjeként értesítési kötelezettség teljesítése. Az érintett adatok tárolásának időtartama: az adatkezelő által nyújtott szolgáltatások igénybe vételének időtartamát követő 5 éven belül. A szolgáltatások igénybe vételét követő adatkezelés a számlák és a teljesítés igazolásának ellenőrzési idejére tekintettel szükséges. Adattovábbítás: - számlaadatok könyvelő részére. - úszásoktatás helyszínét biztosító uszoda részére. Szerződő partnerek adatainak kezelése – vevők, szállítók nyilvántartása

3.5 Szerződő partnerek adatainak kezelése – vevők, szállítók nyilvántartása A Társaság szerződés teljesítése jogcímén a szerződés megkötése, teljesítése, megszűnése, szerződési kedvezmény nyújtása céljából kezeli a vele vevőként, szállítóként szerződött természetes személy nevét, születési nevét, születési idejét, anyja nevét, lakcímét, adóazonosító jelét, adószámát, vállalkozói, őstermelői igazolvány számát, személyi igazolvány számát, lakcímét, székhely, telephely címét, telefonszámát, e-mail címét, honlap-címét, bankszámlaszámát, vevőszámát (ügyfélszámát, rendelésszámát), online azonosítóját (vevők, szállítók listája, törzsvásárlási listák), Ezen adatkezelés jogszerűnek minősül akkor is, ha az adatkezelés a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges. A személyes adatok címzettjei: a Társaság ügyfélkiszolgálással kapcsolatos feladatokat ellátó munkavállalói, könyvelési, adózási feladatokat ellátó munkavállalói, és adatfeldolgozói. A személyes adatok tárolásának időtartama: a szerződés megszűnését követő 5 év. Az érintett természetes személlyel az adatkezelés megkezdése előtt közölni kell, hogy az adatkezelés a szerződés teljesítése jogcímén alapul, az a tájékoztatás történhet a szerződésben is. Az érintettet személyes adatai adatfeldolgozó részére történő átadásáról tájékoztatni kell.

3.6 Jogi személy ügyfelek, vevők, szállítók természetes személy képviselőinek elérhetőségi adatai A kezelhető személyes adatok köre: a természetes személy neve, címe, telefonszáma, e-mail címe, online azonosítója. A személyes adatok kezelésének célja: a Társaság jogi személy partnerével kötött szerződés teljesítése, üzleti kapcsolattartás, jogalapja: az érintett hozzájárulása. A személyes adatok címzettjei, illetve a címzettek kategóriái: a Társaság üzleti partnerrel, szerződés teljesítésével kapcsolatos feladatokat ellátó munkavállalói. A személyes adatok tárolásának időtartama: az üzleti kapcsolat, illetve az érintett képviselői minőségének fennállását követő 5 évig.

4. A Társaság adatvédelmi rendszere A Társaság mindenkori vezető tisztségviselője a Társaság sajátosságainak figyelembevételével meghatározza az adatvédelem szervezetét, az adatvédelemre, valamint az azzal összefüggő tevékenységre vonatkozó feladat- és hatásköröket, és 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 vezető tisztségviselő látja el, aki jogosult adatvédelmi tisztviselőt kinevezni. Az adatvédelmi tisztviselőt szakmai rátermettség, az adatvédelmi jog és gyakorlat szakértői szintű ismerete alapján kell kinevezni. Amennyiben sor kerül adatvédelmi tisztviselő kinevezésére, úgy a Társaság biztosítja az adatvédelmi tisztviselő részére a feladat ellátásához szükséges forrásokat, valamint biztosítja számára, hogy a feladatai ellátása során utasításokat senkitől ne fogadjon el, ezen feladatai ellátásával összefüggésben nem bocsátható el és szankcióval nem sújtható. Az adatvédelmi tisztviselő szervezetileg közvetlenül a Társaság vezető tisztségviselőjének tartozik felelősséggel. Az adatvédelmi tisztviselő a vezető tisztségviselő közvetlen felügyeletével szervezi, irányítja és ellenőrzi a Társaság adatvédelmi és adatbiztonsági rendszerét. Az adatvédelmi tisztviselő a Társaság saját alkalmazottja. Felette a munkáltatói vagy szerződésben meghatározott jogokat a Társaság vezető tisztségviselője gyakorolja. A Társaság vezető tisztségviselője az adatvédelemmel kapcsolatosan: a) felelős az érintettek Infotv.-ben 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 az adatvédelmi tisztviselő tevékenységét; e) vizsgálatot rendelhet el; f) kiadja a Társaság adatvédelemmel kapcsolatos belső szabályait. Az adatvédelmi tisztviselő adatvédelemmel kapcsolatos feladatai: a) segítséget nyújt az érintett jogainak biztosításában; b) kezdeményezi NAIH felé az Infotv.-ben meghatározott nyilvántartásba vételi eljárás lefolytatását; c) minden év január 15-ig jelentést készít a vezető tisztségviselő részére a Társaság adatvédelmi feladatainak végrehajtásáról; d) jogosult jelen szabályzat betartását az egyes szervezeti egységeknél ellenőrizni; e) vezeti az adattovábbítási nyilvántartást; f) részt vesz a NAIH által szervezett adatvédelmi tisztviselők konferenciáján; g) figyelemmel kíséri az adatvédelemmel és információszabadsággal kapcsolatos jogszabályváltozásokat, ezek alapján indokolt esetben kezdeményezi jelen szabályzat módosítását; h) közreműködik a NAIH-tól a Társasághoz érkezett megkeresések megválaszolásában és a NAIH által kezdeményezett vizsgálat, illetve adatvédelmi hatósági eljárás során; i) általános állásfoglalás megadása céljából megkeresést fogalmaz meg a NAIH felé, amennyiben egy felmerült adatvédelmi kérdés jogértelmezés útján egyértelműen nem válaszolható meg; j) tájékoztatást és szakmai tanácsot ad a Társaság adatvédelmi jogszabályokban előírt kötelezettségeinek ellátásával kapcsolatban; k) ellenőrzi az adatvédelmi jogszabályoknak, valamint a Társaság belső szabályzatainak való megfelelést, ideértve a feladatkörök kijelölését, az adatkezelési műveletekben résztvevő személyek tudatosság-növelését és képzését, valamint a kapcsolódó auditokat is; l) kérésre szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, valamint nyomon követi a hatásvizsgálat elvégzését; m) együttműködikaNAIH-val; n) az adatkezeléssel összefüggő ügyekben kapcsolattartó pontként szolgál a NAIH felé, valamint bármely egyéb kérdésben konzultációt folytat le.

5. Adatvédelmi incidens kezelése Adatvédelmi incidens észlelése és jelentése A Társaság minden munkavállalója – beleértve az egyéb jogviszonyban foglalkoztatott személyeket is – köteles a Társaságon belül történt adatvédelmi incidenst haladéktalanul jelenteni a szervezeti egysége vezetőjének, a Társaság ügyvezetőjének, illetve amennyiben kijelölésre kerül, úgy az adatvédelmi tisztviselőnek. A bejelentés tartalmazza a bejelentő nevét, telefonszámát, beosztását, szervezeti egységének megnevezését, valamint az incidens tárgyát, rövid leírását és azt, hogy az incidens érinti-e a Társaság informatikai rendszerét. A bejelentés az ügyvezetőhöz vagy az adatvédelmi tisztviselőhöz érkezését követően az ügyvezető vagy az adatvédelmi tisztviselő haladéktalanul megkezdi az adatvédelmi incidens kivizsgálását és értékelését. Adatvédelmi incidens kivizsgálása, értékelése Az ügyvezető vagy az adatvédelmi tisztviselő megvizsgálja a bejelentést és amennyiben szükséges, a bejelentőtől további adatokat kér az incidensre vonatkozóan. Az ügyvezető vagy az adatvédelmi tisztviselő felhívására a bejelentő köteles megadni: az adatvédelmi incidens bekövetkezésének időpontját és helyét, az adatvédelmi incidens egyéb körülményeit, az adatvédelmi incidens által érintett adatok körét, mennyiségét, az adatvédelmi incidenssel érintett személyek körét és számát, az adatvédelmi incidens várható hatásait, az adatvédelmi incidens megelőzésére, következményeinek enyhítésére megtett intézkedések felsorolását. A bejelentő az adatszolgáltatást haladéktalanul, de legkésőbb 2 munkanapon belül teljesíti az ügyvezető vagy az adatvédelmi tisztviselő részére. Amennyiben az adatvédelmi incidens értékelése vizsgálatot igényel az ügyvezető vagy adatvédelmi tisztviselő egyéb, a vizsgálat lefolytatásához szükséges munkatársak bevonásával lefolytatja a vizsgálatot. A vizsgálatnak tartalmaznia kell, hogy az adatvédelmi incidens magas kockázattal jár-e az érintettek jogaira és kötelezettségeire, milyen jellegű kockázatról van szó és szükséges-e az érintettek tájékoztatása az incidensről. Amennyiben nem szükséges az érintettek tájékoztatása, a vizsgálatnak tartalmazni kell ennek indokait is. A vizsgálat eredményeként javaslatot kell készíteni az incidens kezeléshez szükséges intézkedések megtételére. A javaslat alapján a megvalósítandó további intézkedésekről a vezető tisztségviselő dönt. A vizsgálatot legkésőbb a bejelentés adatvédelmi tisztviselőhöz érkezésétől számított három munkanapon belül be kell fejezni és a vizsgálat eredményéről a Társaság vezető tisztségviselőjét az adatvédelmi tisztviselő tájékoztatja. Az adatvédelmi incidens nyilvántartása Az adatvédelmi incidensről az adatvédelmi tisztviselő nyilvántartást vezet. A nyilvántartás tartalmazza: • az érintett személyes adatok körét, • az adatvédelmi incidenssel érintettek körét és számát, • az adatvédelmi incidens időpontját, • az adatvédelmi incidens körülményeit, hatásait, • az elhárítására megtett intézkedéseket és • egyéb jogszabályban előírt adatokat. Az adatvédelmi incidens nyilvántartás pontos vezetéséről, aktualizálásáról az adatvédelmi tisztviselő gondoskodik. Az adatvédelmi incidens bejelentése a Hatóság részére Az adatvédelmi tisztviselő az adatvédelmi incidenst, a bekövetkezését követően haladéktalanul, de legkésőbb az incidens észlelésétől számított hetvenkét (72) órán belül bejelenti a Hatóság részére, kivéve, ha az incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Ha a bejelentés nem történik meg határidőben, az adatvédelmi tisztviselő köteles ennek okát igazolni a Hatóság részére. A Hatósági bejelentésnek tartalmaznia kell: • az adatvédelmi incidenssel érintett adatok körét és hozzávetőleges számát, • az adatvédelmi incidenssel érintett személyek körét és hozzávetőleges számát, • az adatvédelmi incidens jellegét, körülményeit, • az adatvédelmi tisztviselő nevét és elérhetőségét, • az adatvédelmi incidens valószínűsíthető következményeit és • az adatvédelmi incidens orvoslására és enyhítésére megtett intézkedéseket. Az érintettek tájékoztatása az adatvédelmi incidensről Ha a vizsgálat eredményeként megállapítást nyert, hogy az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságára nézve és az érintettek tájékoztatása szükséges, az adatvédelmi tisztviselő haladéktalanul értesíti az érintetteket és erről a Társaság vezető tisztségviselőjét is értesíti. Nem kell az érintetteket tájékoztatni: • ha a Társaság olyan technikai, szervezési, védelmi intézkedéseket hajtott végre az érintett adatokra vonatkozóan, amelyek megakadályozzák az illetéktelen személyek számára való hozzáférést az adatokhoz vagy megakadályozzák az adatok értelmezhetőségét. • ha az adatvédelmi incidens bekövetkezését követően a Társaság olyan intézkedéseket tett, amelyek biztosítják, hogy a feltárt adatkezelési kockázat valószínűsíthetően nem valósul meg. • ha a tájékoztatás aránytalan erőfeszítést tenne szükségessé. Ebben az esetben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, mely tájékoztatás elektronikus úton is megtörténhet.

6. Adatbiztonsági szabályok Fizikai védelem A papíralapon kezelt személyes adatok biztonsága érdekében a Társaság az alábbi intézkedéseket alkalmazza: • az adatokat csak az arra jogosultak ismerhetik meg, azokhoz más nem férhet hozzá, más számára fel nem tárhatók; • a dokumentumokat jól zárható, száraz, tűzvédelmi és vagyonvédelmi berendezéssel ellátott helyiségben helyezi el; • a folyamatos aktív kezelésben lévő iratokhoz csak az illetékesek férhetnek hozzá; • 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. Amennyiben a papíralapon tárolt személyes adat kezelésének célja megvalósult, úgy a Társaság intézkedik a papír megsemmisítéséről. Ebben az esetben a Társaság kijelöl egy munkavállalót, aki a megsemmisítésért felelős. A megsemmisítésért felelős munkavállaló a megsemmisítéssel érintett szervezeti egység bevonásával állítja össze a megsemmisítendő iratcsomagot. A megsemmisítésen háromtagú megsemmisítési bizottság vesz részt. Amennyiben a személyes adatok adathordozója nem papír, hanem más fizikai eszköz, úgy a fizikai eszköz megsemmisítésére a papíralapú dokumentumokra vonatkozó megsemmisítési szabályok az irányadóak. Informatikai védelem A számítógépen, illetve hálózaton tárolt személyes adatok biztonsága érdekében a Társaság 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 csak hozzáférni, a jelszavak cseréjéről Társaság rendszeresen, illetve indokolt esetben 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 szerverek esetén magas rendelkezésre állású infrastruktúrán történik mentésekkel és archiválással 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. Jogosultságkezelés A jogosultságkezelés szabályozásának célja, hogy a kiosztott jogosultságok pontosan nyomon követhetőek legyenek, dokumentált formában megőrzésre kerüljenek, valamint az egyes jogosultságokkal rendelkező személyek tevékenysége és az általuk felhasznált adatok köre ellenőrizhető legyen. Ezen adatok naprakészsége nagymértékben hozzásegíti a Társaságot a tőle elvárt, illetve általa elérhető biztonsági szint teljesítéséhez, továbbá az informatikai hálózat törvényi és szakmai normák szerinti üzemeltetéséhez. A szabályozás kiterjed az elektronikus megfigyelőrendszerek informatikai rendszerére és az azokhoz csatlakozó eszközökre. Az informatikai rendszerben a jogosultságok változásait (létező jogosultságok, új jogosultságok kiosztása, módosítása, megszűnése) dokumentálni kell. A személyes adatok biztonsága érdekében a Társaság az alábbi jogosultságkezelési előírásokat alkalmazza: • Alapelvek o Új jogosultság beállítását, illetve jogosultság megváltoztatását a jogosultság birtokosának felhatalmazása alapján a vezető tisztségviselő végzi. o A jogosultságok megállapítása során kizárólag a munkavégzéshez szükséges és elégséges jogosultságokat kell kiosztani. o El kell kerülni, hogy teljes hozzáférést, illetve adminisztrátori jogosultságokat kapjanak más munkát végző, illetve a jogosultság birtoklására igényt nem tartó személyek. o Adminisztrátori jogosultsággal rendelkező nevesített felhasználót kell alkalmazni a rendszer adminisztrálása érdekében minden esetben, ahol ez lehetséges. A nem nevesített rendszergazdai jelszavakat zárt borítékban, felbontást gátló módon, aláírva kell tárolni. Ezek használatát az Adatkezelő vezető tisztségviselője vagy akadályoztatása esetén helyettesítési rend szerinti helyettese engedélyezheti. A nem nevesített felhasználói jogosultságok használatát indokolni

és dokumentálni kell. o Külső – karbantartó vagy fejlesztő – cég alkalmazottja folyamatosan működő, korlátlan időre szóló hozzáférési jogosultsággal nem rendelkezhet.

7. Álnevesítés Az álnevesítés a személyes adatok olyan módon történő kezelése, amelynek következtében további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik, mivel a Társaság az ilyen további információt külön tárolja, és technikai és szervezési intézkedések megtételével biztosítja, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet kapcsolni. Az álnéven történő adatkezelést a Társaság a nagyobb fokú biztonság érdekében, valamint a statisztikai célra gyűjtendő adatok vagy a fejlesztés, tesztelés, karbantartás alatt álló rendszerek esetében a tesztadatok tekintetében végez, mivel a személyes adatok álnevesítése csökkentheti az érintettek számára a kockázatokat, valamint a Társaság ezáltal könnyebben meg tud felelni az adatvédelmi kötelezettségeinek. Az álnevesítés személyes adatok kezelése során történő alkalmazásának ösztönzése céljából lehetővé teszi az álnevesítésre irányuló intézkedések és az általános elemzés egyidejű alkalmazását a Társaság szervezetén belül. A Társaság továbbá biztosítja, hogy az ahhoz szükséges további információkat, amelyek által a személyes adatokat egy adott érintetthez lehessen kapcsolni, elkülönítve tárolják. A Társaságnál az adatvédelmi tisztviselő az, aki ugyanazon a szervezeten belül feljogosított személynek minősül. A természetes személyeket személyes adataik kezelése tekintetében megillető jogok és szabadságok védelme megköveteli a Rendelet követelményeinek teljesítését biztosító megfelelő technikai és szervezési intézkedések meghozatalát. Ahhoz, hogy az Adatkezelő igazolni tudja a Rendeletnek való megfelelést, olyan belső szabályokat kell alkalmaznia, valamint olyan intézkedéseket kell végrehajtania, amelyek teljesítik különösen a beépített és az alapértelmezett adatvédelem elveit. A Társaság törekszik - a GDPR-nak való megfelelés érdekében - a személyes adatok kezelésének minimálisra csökkentésére, a személyes adatok mihamarabbi álnevesítésére, a személyes adatok funkcióinak és kezelésének átláthatóságára, valamint arra, hogy az érintett nyomon követhesse az adatkezelést, a Társaság pedig biztonsági elemeket hozhasson létre és továbbfejleszthesse azokat.

8. Beépített adatvédelem Bevezetésre kerül az ún. beépített adatvédelem (privacy by design), melynek következtében a Társaság már az adatkezelés tényleges megkezdése előtt – például már a projekt-előkészítés időszakában – is figyelemmel van a GDPR előírásaira. A beépített adatvédelem a Társaság saját, olyan belső eljárásainak az összessége, amivel - a külső szabályozásoktól függetlenül is - igyekszik megfelelni annak, hogy az érintett magánszféráját minél jobban védje. A természetes személyeket személyes adataik kezelése tekintetében megillető jogok és szabadságok védelme megköveteli a GDPR követelményeinek teljesítését biztosító megfelelő technikai és szervezési intézkedések meghozatalát. Az említett intézkedések magukban foglalják a személyes adatok kezelésének minimálisra csökkentését, a személyes adatok mihamarabbi álnevesítését, a személyes adatok funkcióinak és kezelésének átláthatóságát, valamint azt, hogy az érintett nyomon követhesse az adatkezelést, a Társaság pedig biztonsági elemeket hozzon létre és tovább fejleszthesse azokat. Az adatkezelésnek átláthatónak és felhasználó-központúnak, az adatvédelemnek pro-aktívnak kell lennie, és az adat teljes életciklusát fel kell ölelnie, vagyis a teljes folyamatnak része kell, hogy legyen. A Társaság a tudomány és a technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével, mind az adatkezelés módjának meghatározásakor, mind pedig az adatkezelés során olyan megfelelő technikai és szervezési intézkedéseket – a) a személyes adatok álnevesítését és titkosítását; b) a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítását, integritását, rendelkezésre állását és ellenálló képességét; c) fizikai vagy műszaki incidens esetén az arra való képességet, hogy a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását kellő időben vissza lehet állítani; d) az adatkezelés biztonságának garantálására hozott technikai és szervezési intézkedések hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárást - hajt végre, amelyek célja egyrészt az adatvédelmi elvek, például az adattakarékosság hatékony megvalósítása, másrészt a GDPR-ban foglalt követelmények teljesítéséhez és az érintettek jogainak védelméhez szükséges garanciák beépítése az adatkezelés folyamatába. A Társaság

megfelelő technikai és szervezési intézkedéseket hajt végre annak biztosítására, hogy alapértelmezés szerint kizárólag olyan személyes adatok kezelésére kerüljön sor, amelyek az adott konkrét adatkezelési cél szempontjából szükségesek. Ez a kötelezettség vonatkozik a gyűjtött személyes adatok mennyiségére, kezelésük mértékére, tárolásuk időtartamára és hozzáférhetőségükre. Ezek az intézkedések különösen azt kell, hogy biztosítsák, hogy a személyes adatok alapértelmezés szerint a természetes személy beavatkozása nélkül ne válhassanak hozzáférhetővé meghatározatlan számú személy számára. A GDPR 42. cikke szerinti jóváhagyott tanúsítási mechanizmus felhasználható annak bizonyítása részeként, hogy a Társaság teljesíti az előbbiekben előírt követelményeket. A Társaság és az adatfeldolgozó intézkedéseket hoz annak biztosítására, hogy a Társaság vagy az adatfeldolgozó irányítása alatt eljáró, a személyes adatokhoz hozzáféréssel rendelkező természetes személyek kizárólag a Társaság utasításának megfelelően kezelhessék az említett adatokat, kivéve, ha az ettől való eltérésre uniós vagy tagállami jog kötelezi őket. A beépített és az alapértelmezett adatvédelem elveit a közbeszerzések során is figyelembe veszi a Társaság. Adattovábbítás esetén a megfelelőségi határozat hiányában a Társaság vagy az adatfeldolgozó a megfelelő garanciák érintett számára való biztosítása útján gondoskodik az adatvédelem harmadik országbeli hiányosságainak ellensúlyozásáról. A garanciák biztosítják az adatvédelmi követelményeknek való megfelelést, és az Európai Unión belüli adatkezelés esetén biztosított jogokkal azonos szintű jogokat biztosítanak az érintettek számára, beleértve az érintettek jogainak érvényesíthetőségét és a hatékony jogorvoslat lehetőségét, ezen belül ideértve azt, hogy az érintettek hatékony közigazgatási vagy bírósági jogorvoslatot vehessenek igénybe és kártérítést igényelhessenek az Európai Unióban vagy egy harmadik országban. A garanciák különösen a személyes adatok kezelésére vonatkozó általános elveknek, valamint a beépített és alapértelmezett adatvédelem elveinek való megfelelésre vonatkoznak.

9. Az érintettek jogainak érvényesítése Az érintett tájékoztatást kérhet személyes adatai kezeléséről, valamint kérheti személyes adatainak helyesbítését, illetve – a jogszabályban elrendelt adatkezelések kivételével – törlését, korlátozását a Társaság feltüntetett elérhetőségein. Az érintett jogosult arra, hogy a rá vonatkozó, általa az Adatkezelő rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formában megkapja, továbbá jogosult arra, hogy ezeket az adatokat egy másik adatkezelőnek továbbítsa. A Társaság a beérkezett kérelmet, illetve tiltakozást köteles a beérkezéstől számított három napon belül áttenni az adatkezelés szempontjából feladat- és hatáskörrel rendelkező szervezeti egység vezetőjéhez. A feladat- és hatáskörrel rendelkező szervezeti egység vezetője az érintett személyes adatának kezelésével összefüggő kérelmére az érkezésétől számított legkésőbb 25 – tiltakozási jog gyakorlása esetén 15 – napon belül írásban, közérthető formában választ ad. A tájékoztatás kiterjed az Infotv. 15. § (1) bekezdésében meghatározott információkra, amennyiben az érintett tájékoztatása törvény alapján nem tagadható meg. A tájékoztatás főszabály szerint ingyenes, költségtérítést a Társaság csak az Infotv. 15. § (5) bekezdésében meghatározott esetben számíthat fel. A Társaság kérelmet csak az Infotv. 9. § (1) bekezdésében vagy a 19. §-ában meghatározott okokból utasít el, erre csak indoklással, az Infotv. 16. § (2) bekezdésében meghatározott tájékoztatással, írásban kerül sor. A valóságnak nem megfelelő adatot, az adatot kezelő szervezeti egység vezetője – amennyiben a szükséges adatok és az azokat bizonyító közokiratok rendelkezésre állnak – helyesbíti, az Infotv. 17. § (2) bekezdésében meghatározott okok fennállása esetén intézkedik a kezelt személyes adat törlése iránt. Az érintett személyes adata kezelése elleni tiltakozásának elbírálásának időtartamára – de legfeljebb öt (5) napra – az adatkezelést, az adatkezelést végző szervezeti egység vezetője felfüggeszti, a tiltakozás megalapozottságát megvizsgálja, és döntést hoz, amelyről a kérelmezőt az Infotv. 21. § (2) bekezdésében foglaltak szerint tájékoztatja. Amennyiben a tiltakozás indokolt, az adatot kezelő szervezeti egység vezetője az Infotv. 21. § (3) bekezdésében meghatározottak szerint jár el. Amennyiben az érintett jogainak gyakorlása során az ügy megítélése nem egyértelmű, az adatot kezelő szervezeti egység vezetője az ügy iratainak és az ügyre vonatkozó álláspontjának megküldésével állásfoglalást kérhet az adatvédelmi tisztviselőtől, aki azt három napon belül teljesíti. 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. Az Adatkezelő 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 jogorvoslati lehetőséggel, panasszal a Nemzeti Adatvédelmi és Információszabadság Hatóságnál (1125 Budapest, Szilágyi Erzsébet fasor 22/C.) vagy lakóhelye, vagy tartózkodási helye szerint illetékes törvényszéknél élhet.

10. Az adatkezelő és adatfeldolgozók köre Az adatkezelő Név: Süli Richard
Székhelye és postai címe: 2241 Sülysáp Széchenyi utca 18. Adószáma: 66530642-1-33
E-mail címe: suli.richard@gmail.Com
Könyvelést végző vállalkozás neve: Számlaflotta Kft.

Az adatkezelés jogalapja 1. Személyes adat akkor kezelhető, ha ahhoz az érintett hozzájárul, vagy azt törvény vagy - törvény felhatalmazása alapján, az abban meghatározott körben - helyi önkormányzat rendelete közérdeken alapuló célból elrendeli. 2. Az adatkezelés jogalapja az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Avtv.) 5. § (1) a) bekezdése alapján az érintett önkéntes hozzájárulása, illetve az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény 13/A. §-ában foglaltak. 3. Cselekvőképtelen és korlátozottan cselekvőképes kiskorú személy nyilatkozatához a törvényes képviselőjének hozzájárulása szükséges, kivéve azon szolgáltatás részeket, ahol a nyilatkozat a mindennapi életben tömegesen előforduló regisztrációt céloz, és különösebb megfontolást nem igényel. A 16. életévét betöltött kiskorú érintett hozzájárulását tartalmazó jognyilatkozatának érvényességéhez törvényes képviselőjének beleegyezése vagy utólagos jóváhagyása nem szükséges. 4. Ha a személyes adat felvételére az érintett hozzájárulásával került sor, az adatkezelő a felvett adatokat törvény eltérő rendelkezésének hiányában 4.1. a rá vonatkozó jogi kötelezettség teljesítése céljából, vagy 4.2. az adatkezelő vagy harmadik személy jogos érdekének érvényesítése céljából, ha ezen érdek érvényesítése a személyes adatok védelméhez fűződő jog korlátozásával arányban áll 4.3. további külön hozzájárulás nélkül, valamint az érintett hozzájárulásának visszavonását követően is kezelheti. 4.4. Az adatkezelések jogalapja GDPR szerint: - GDPR 6.cikk (1) bekezdés a) pont: érintett hozzájárulása - GDPR 6.cikk (1) bekezdés b) pont: szerződés teljesítéséhez szükséges - GDPR 6.cikk (1) bekezdés c) pont: jogi kötelezettség teljesítéséhez szükséges - GDPR 6.cikk (1) bekezdés a) pont: jogos érdek, mindig érdekmérlegelés szükséges 4.5. Az egyes adatkezelési tevékenységek jogalapja: - a számviteli jogszabályoknak megfelelő számlát kiállítása: jogalap: GDPR 6. cikk (1) bekezdés c) pont - kapcsolattartás: jogalap (a partnerek munkavállalóinak adatai esetében az adatkezelés) jogalapja: GDPR 6. cikk (1) bekezdés f) pont. Az adatkezelő jogos érdeke: üzletmenet folytonosság. - munkavállalók adatainak kezelése: GDPR 6. cikk (1) bekezdés b), c) pontok. - szerződéses partnerek adatainak kezelése: jogalap GDPR 6. cikk (1) bekezdés b) pont - marketing tevékenység: jogalap: GDPR 6. cikk (1) bekezdés a) pont. - Marketing tevékenység céljából facebook oldal is üzemel, azonban önálló adatbázis létrehozása, profilalkotás nem történik. - on-line regisztráció jogalap: GDPR 6. cikk (1) bekezdés a) pont - biztonsági kamera üzemeltetése jogalap: GDPR 6. cikk (1) bekezdés f) pont. Az adatkezelő jogos érdeke: vagyonvédelem, munkavállalók esetében az Mt.-ben meghatározott munkáltatói jogos érdek. 12. A felhasználó jogai 1. A Társaság tájékoztatja az érintettet, hogy az általa kezelt személyes adatait az adatkezelésre- és feldolgozásra jogosult, jelen tájékoztatóban rögzített személyhez történő előzetes bejelentkezést követően megismerheti, azokba betekintést nyerhet. 2. A Társaság tájékoztatja az érintettet, hogy a hozzájáruláson alapuló adatainak kezeléséhez adott hozzájárulását a Társaság részére írásban megküldött értesítéssel bármikor visszavonhatja. 3. Amennyiben az érintett az adatkezeléssel - így különösen, de nem kizárólagosan az adatbiztonsággal - kapcsolatos rendelkezések megsértését észleli jogosult közvetlenül a Társasághoz fordulni a jogellenes gyakorlat megszűntetése érdekében. 4. Amennyiben a jogellenes gyakorlatot a Társaság az érintett kifejezett felhívása ellenére nem szűnteti meg, úgy az érintett bírósági úton kérheti a Társaságot kötelezni a jogellenes gyakorlat megszűntetésére, egyúttal kérheti az adatkezelési szabályok megsértésével okozati összefüggésben keletkezett kárai megtérítését