

A First Choice Hungary Kft.
szabályzata

az adatkezelésekről, adatbiztonságról,
valamint
az adatvédelmi incidensek kezeléséről

Hatályos: 2018. május 25. napjától

I. A szabályzat célja és hatálya

I.1. A jelen szabályzat célja, hogy First Choice Hungary Kft. (a továbbiakban: „**Adatkezelő**”) által személyes adatokon végzett adatkezelés során

a) a jogszerű adatkezeléshez szükséges feltételeket megteremtse

b) a személyes adatok jogosulatlan felhasználásának megakadályozása érdekében adatvédelmi és adatbiztonsági előírásokat határozzon meg;

c) adatvédelmi incidens esetén az Adatkezelő megfelelő és hatékony intézkedéseket hozzon az adatkezelés biztonságának további sérülése ellen, valamint megfelelően minimalizálja a bekövetkezett károkat, és az Európai Parlament és a Tanács (EU) 2016/679 Rendelete (2016. április 27.) 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 (a továbbiakban: „**GDPR**”) előírásainak megfelelően tájékoztassa az incidensről a Nemzeti Adatvédelmi és Információszabadság Hatóságot és az érintetteket.

I.2. A Jelen szabályzat tárgyi hatálya kiterjed az Adatkezelő által végzett valamennyi olyan adatkezelésre, amelynek során személyes adatok kezelése történik, függetlenül a személyes adatok jellegétől vagy az érintettek körétől.

I.3. A jelen szabályzat személyi hatálya kiterjed az Adatkezelő valamennyi munkavállalójára, továbbá - az adatfeldolgozói szerződések ilyen rendelkezése esetén – az Adatkezelővel szerződéses viszonyban álló adatfeldolgozókra.

II. Értelmező rendelkezések

A jelen szabályzat alkalmazásában:

1. „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;

2. „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;

3. „az adatkezelés korlátozása”: a tárolt személyes adatok megjelölése jövőbeli kezelésük korlátozása céljából;

4. „profilalkotás”: 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 előre jelzésére használják;

5. „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, 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;

6. „nyilvántartási rendszer”: a személyes adatok bármely módon – centralizált, decentralizált vagy funkcionális vagy földrajzi szempontok szerint – tagolt állománya, amely meghatározott ismérvek alapján hozzáférhető;

7. „adatkezelő”: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza; ha az adatkezelés céljait és eszközeit az uniós vagy a tagállami jog határozza meg, az adatkezelőt vagy az adatkezelő kijelölésére vonatkozó különös szempontokat az uniós, vagy a tagállami jog is meghatározhatja;

8. „adatfeldolgozó”: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az Adatkezelő nevében személyes adatokat kezel;

9. „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 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 meg-felelően az alkalmazandó adatvédelmi szabályoknak;

10. „harmadik fél”: 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;

11. „az érintett hozzájárulása”: az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel az érintett nyilatkozik vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez;

12. „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;

13. „egészségügyi adat”: 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;

14. „érintett”: az a természetes személy, akinek a személyes adatait az Adatkezelő vagy az adatfeldolgozó kezeli.

III. Az adatkezelés alapelvei, jogalapja

III.1

A személyes adatok védelméhez való jog a természetes személyek Alaptörvényben biztosított alapjoga, amely garantálja az adatalanyok információs önrendelkezési jogát. Az információs önrendelkezési jog az érintettek beleegyezésének hiányában kizárólag törvényi felhatalmazás alapján korlátozható.

Az információs önrendelkezési jog tiszteletben tartása érdekében személyes adatot kezelni csak a GDPR 6. cikkének (1) bekezdésében meghatározott következő esetekben lehet:

- 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 az Adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges;
- d) az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges;
- e) az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges;
- f) az adatkezelés az Adatkezelő 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.

III.2. Az adatkezelés jogalapját az alábbi esetkörök képezhetik:

III.2.a. Az érintett hozzájárulása

- (1) A személyes adatok kezelése jogszerűségének az érintett hozzájárulásán kell alapulnia, vagy valamely egyéb jogszerű, jogszabály által megállapított alappal kell rendelkeznie.
- (2) Az érintett hozzájárulása alapján történő adatkezelés esetén az érintett a személyes adatainak kezeléséhez való hozzájárulását a következő formában adhatja meg:
 - a) írásban, személyes adatkezeléshez hozzájárulást adó nyilatkozási formában,
 - b) elektronikus úton, a Vállalkozás internetes weboldalán megvalósított kifejezett magatartásával, jelölőnégyzet kipipálásával, vagy ha az információs társadalommal összefüggő szolgáltatások igénybevétele során erre vonatkozó technikai beállításokat hajt végre, valamint bármely egyéb olyan nyilatkozat vagy cselekedet is, amely az adott összefüggésben az érintett hozzájárulását személyes adatainak tervezett kezeléséhez egyértelműen jelzi.
- (3) A hallgatás, az előre bejelölt négyzet vagy a nem cselekvés ezért nem minősül hozzájárulásnak.
- (4) A hozzájárulás az ugyanazon cél vagy célok érdekében végzett összes adatkezelési tevékenységre kiterjed.
- (5) Ha az adatkezelés egyszerre több célt is szolgál, akkor a hozzájárulást az összes adatkezelési célra vonatkozóan meg kell adni. Ha az érintett hozzájárulását elektronikus felkérést követően adja meg, a felkérésnek egyértelműnek és tömörnek kell lennie, és az nem gátolhatja szükségtelenül azon szolgáltatás igénybevételét, amely vonatkozásában a hozzájárulást kérik.
- (6) Az érintett jogosult arra, hogy hozzájárulását bármikor visszavonja. A hozzájárulás visszavonása nem érinti a hozzájáruláson alapuló, a visszavonás előtti adatkezelés jogszerűségét. A hozzájárulás megadása előtt az érintettet erről tájékoztatni kell. A hozzájárulás visszavonását ugyan-olyan egyszerű módon kell lehetővé tenni, mint annak megadását.
A gyermekek személyes adatai különleges védelmet érdemelnek, mivel ők kevésbé lehetnek tisztában a személyes adatok kezelésével összefüggő kockázatokkal, következményeivel és az ahhoz kapcsolódó garanciákkal és jogosultságokkal. A 16. életévét be nem töltött gyermek esetén, a gyermekek személyes adatainak kezelése csak akkor és olyan mértékben jogszerű, ha a hozzájárulást a gyermek szülői felügyeletet gyakorló adta meg, illetve engedélyezte. Adatkezelő - figyelembe véve az elérhető technológiát – ésszerű erőfeszítéseket tesz, hogy ilyen esetekben ellenőrizze, hogy a hozzájárulást a gyermek feletti szülői felügyeleti jog gyakorlója adta meg, illetve engedélyezte.

III.2.b. Szerződés teljesítése

- (1) Az adatkezelés jogszerűnek minősül, ha az olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél, vagy az a szerződés megkötését megelőzően az érintett kérésére

történő lépések megtételéhez szükséges.

(2) A szerződés teljesítéséhez nem szükséges személyes adatok kezeléséhez való érintett hozzájárulás nem lehet feltétele a szerződéskötésnek.

III.2.c. Jogos érdek

(1) Az adatkezelés jogalapját jogi kötelezettség teljesítése esetén törvény határozza meg, így az érintett hozzájárulása a személyes adatainak kezeléséhez nem szükséges.

(2) Az adatkezelő köteles tájékoztatni az érintettet az adatkezelés céljáról, jogalapjáról, időtartamáról az adatkezelő személyéről, továbbá a jogairól, a jogorvoslati lehetőségekről.

(3) Az adatkezelő jogi kötelezettség teljesítése címén az érintett hozzájárulásának visszavonását követően jogosult kezelni azon adatkört, amely valamely rá vonatkozó jogi kötelezettség teljesítése végett szükséges.

III.2. A személyes adatok kezelésére vonatkozó elvek:

- a) személyes adatokat jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell kezelni.
- b) A személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból, tehát célhoz kötötten történhet.
- c) az adatkezelésnek minden esetben a szükséges mértékre kell korlátozódnia („adattakarékosság”);
- d) a kezelt adatoknak pontosnak, és szükség esetén naprakésznek kell lenniük: minden ésszerű intézkedést meg kell tenni annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatok törlésre vagy helyesbítésre kerüljenek („pontosság”);
- e) a személyes adatok tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé („korlátozott tárolhatóság”);
- f) a személyes adatok kezelését oly módon kell végezni, hogy biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve („integritás és bizalmas jelleg”).

IV. Adatbiztonság

IV.1. Az Adatkezelő, illetve tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek a GDPR szerinti garanciák érvényre juttatásához szükségesek.

IV.2. Az adatokat megfelelő intézkedésekkel védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen.

IV.3. Az Adatkezelő és az adatfeldolgozó által kezelt nyilvántartásokban, az elektronikusan kezelt adatállományok védelme érdekében megfelelő technikai megoldással biztosítani kell, hogy a nyilvántartásokban tárolt adatok - kivéve, ha ehhez az érintett előzetesen hozzájárult - közvetlenül ne legyenek összekapcsolhatók és az érintetthez rendelhetők.

IV.4. A személyes adatok kezelése során biztosítani szükséges:

- a) a jogosulatlan adatbevitel megakadályozását;

- b) az automatikus adatfeldolgozó rendszerek jogosulatlan személyek általi, adatátviteli berendezés segítségével történő használatának megakadályozását;
- c) annak ellenőrizhetőségét és megállapíthatóságát, hogy a személyes adatokat adatátviteli berendezés alkalmazásával mely szervezetnek továbbították vagy továbbíthatják;
- d) annak ellenőrizhetőségét és megállapíthatóságát, hogy mely személyes adatokat, mikor és ki vitte be az automatikus adatfeldolgozó rendszerekbe;
- e) 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.

IV.5. A személyes adatok biztonságos kezelése és őrzése érdekében a munkavállalók a munkaidő végén – vagy amennyiben elhagyják munkaállomásukat a munkaidő alatt - kötelesek gondoskodni arról, hogy személyes adatot tartalmazó okirat, egyéb dokumentum, adathordozó az asztalukon vagy egyébként a munkaállomásukon őrizet nélkül ne maradjon. A személyes adatokat tartalmazó adathordozókat – a jelen szabályzat eltérő rendelkezése hiányában - a munkaállomásokon, elzárt helyen szükséges őrizni.

IV.6. A munkaszerződéseket és a munkavállalók személyi anyagát tartalmazó adathordozókat, dokumentumokat az irodavezető irodájában, zárt szekrényben szükséges tárolni.

IV.7. Az Adatkezelő székhelyét a munkaidő végén utoljára elhagyó munkatárs köteles az ajtókat bezárni és a riasztót élesíteni.

IV.8. A Szervezet munkatársai felelősek a rendelkezésükre bocsátott információkért, információkezelő és védelmi rendszerek és infokommunikációs eszközök rendeltetésszerű kezeléséért, használatáért. Felelősségre vonhatóak az információ biztonságot sértő cselekedeteikért és anyagi javak (Informatikai eszközök, perifériák) nem rendeltetésszerű használatából eredő meghibásodásaikért.

IV.9. Minden rendellenességet (üzemképtelenség, megváltozott informatikai állapot) haladéktalanul jelenteni kell a rendszergazdának, amennyiben adatvédelmi incidens bekövetkezése valószínűsíthető, az ügyvezetőnek is.

IV.10. Infokommunikációs eszköz (hardver, szoftver) módosítása kizárólag az ügyvezető engedélyével lehetséges.

IV.11. Az Adatkezelő valamennyi munkavállalója köteles bizalmasan és biztonságosan kezelni minden, az Adatkezelő szervezetében, infokommunikációs rendszerében felhasznált adatot, illetve amelyekhez a munkája során a partnerek adataiból hozzáfér, függetlenül attól, hogy azok elektronikusan vagy papíron találhatóak.

IV.12. A munkavállaló a munkaviszonya megszűnésekor köteles visszaszolgáltatni minden nála lévő, az Adatkezelő tulajdonát képező iratot adathordozót és eszközt.

V. Számítógépek és hálózatok használata

V.1. Az Adatkezelő tulajdonában álló számítógépeket csak az arra felhatalmazott alkalmazottak használhatják, akik egyben felelősek azok rendeltetésszerű használatáért. Az Adatkezelő információihoz, infokommunikációs rendszeréhez hozzáférni csak hozzáférési jogosultsággal lehet. A hozzáférési jogosultságok engedélyezéséről, beállításáról, visszavonásáról, törléséről és ellenőrzéséről az ügyvezető dönt.

V.2. A berendezések hibátlan és üzemszerű működésének biztosítása érdekében a számítógépek karbantartását rendszeresen el kell végezni. A gépek karbantartását – a garanciális eszközök kivételével – kizárólag a rendszergazda végezheti.

V.3. Az Adatkezelőnél üzembe helyezett számítógépeken csak előzetesen ellenőrzött és jogtiszt programok futhatnak. Az ellenőrzésnek az esetleges működést akadályozó hibák felderítésén túl ki kell térnie az adatvédelem kérdéskörére is. A feltárt hiányosságokról a program szállítóját írásban kell tájékoztatni. Hibás programot üzembe helyezni tilos. Szoftver telepítésére/frissítésére csak rendszergazda jogosult; a tesztelést a felhasználó és a rendszergazda közösen végzi. Az adatbiztonsági (vírusellenőrzés, adatmentés) célú szoftverek beállításainak módosítása, működésük felfüggesztése még átmenetileg is tilos.

V.4. A számítógépek fizikai meghibásodása vagy rendellenes működése esetén az eszköz használatát fel kell függeszteni, és haladéktalanul értesíteni kell a rendszergazdát.

V.5. Bármilyen külső adathordozó eszköz (pendrive, külső winchester stb.) csatlakoztatása esetén a vírusvédelmi szoftver segítségével először ellenőrizni kell annak vírusmentességét. Amennyiben a használó fertőzött fájlt észlel, az eszköz használata tilos, és haladéktalanul értesíteni kell a rendszergazdát.

V.6. A bizalmas dokumentumokat csak az ügyvezető engedélyével és csak akkor lehet a munkavégzés helyéről eltávolítani, ha azokra okvetlenül külső helyszínen van szükség. Az Adatkezelő informatikai eszközeiről programot, illetve adatállományokat másolni az otthoni munkavégzési célú másoláson és a biztonsági mentéseken kívül tilos.

V.7. Az Adatkezelő számítógépein internet-korlátozás nincs beállítva, ezért a felhasználók fokozott felelősséget viselnek az internethasználat során a jogszabályi előírások és az adatbiztonsági előírások betartásáért.

V.8. Tilos bizonytalan eredetű e-mailek megnyitása, illetve az internetről bármilyen szoftver telepítése. Probléma észlelése vagy rendellenes működés esetén az eszköz használatát fel kell függeszteni, és haladéktalanul értesíteni kell a rendszergazdát

V.9. Valamennyi számítógéphez – beleértve a szervert is – szünetmentes áramforrást kell használni, amely megvédi a berendezést a feszültségingadozásoktól, áramkimaradás esetén az adatvesztéstől.

V.10. A munkavállalók kötelesek a munkaidő végétével számítógépüket és a kapcsolódó eszközöket kikapcsolni, a külső adathordozókat elzárni. Amennyiben munkaállomásukat a munkaidő alatt elhagyják, a munkavállalók kötelesek zárolni számítógépüket.

V.11. A szerver adattartalmának biztonsági mentése naponta megtörténik, ugyanakkor a számítógépek munkavégzéshez szükséges adattartalmáról a munkavállalók kötelesek – legalább heti gyakorisággal biztonsági mentést végezni.

V.12. Az infokommunikációs rendszerbe csak az ügyvezetővel előzetesen egyeztetett eszközök, szoftverek telepíthetőek. A rendszergazda jogosult minden olyan eszközt eltávolítani, amely nem felel meg a biztonsági elvárásoknak vagy nincs engedélyezve annak hálózatra csatlakoztatása.

V.13. A munkaállomás elhagyása esetére kötelező a jelszóhoz kötött feloldású képernyővédő eszközök használata.

VI. Eljárás adatvédelmi incidens esetén

VI.1. Adatvédelmi incidens bekövetkezése esetén az incidenst vagy annak nyomait megfelelően rögzíteni kell, és haladéktalanul tájékoztatni szükséges a bekövetkezett incidensről az ügyvezetőt és egyidejűleg az Adatkezelő valamennyi alkalmazottja köteles megtenni a kárenyhítéshez, illetve a nyomok rögzítéséhez szükséges valamennyi intézkedést, így különösen adatok mentését, helyreállítását kérni az érintett szolgáltatóktól, álnevesítést vagy titkosítást kezdeményezni, az Adatkezelő által üzemeltetett kamerák felvételeit megvizsgálni. A jelen pont szerinti kötelezettségek az adatfeldolgozót is terhelik az általa kezelt személyes adatokkal kapcsolatos incidens esetén.

VI.2. A VI.1. pont szerinti tájékoztatásnak különösen ki kell terjednie az adatvédelmi incidens jellegére, az érintett személyes adatok körére, az érintettek számára, a károsodás, az esetleges illetéktelen hozzáférés súlyosságára, a további lehetséges következményekre és a szükséges további intézkedésekre. A tájékoztatást nem lehet arra figyelemmel késleltetni, hogy további információk szerzése szükséges.

VI.3. Az ügyvezető haladéktalanul köteles részletesen megvizsgálni az adatvédelmi incidenst. Ennek során mindazon személyek, akikre a jelen szabályzat személyi hatálya kiterjed, kötelesek az ügyvezető rendelkezésére állni a vizsgálat során és részletes információkat szolgáltatni.

VI.4. Az ügyvezető az incidens bekövetkezésétől számított 36 órán belül – illetve amennyiben az incidensről való tudomásszerzésre csak később kerül sor, a tudomásszerzéstől számított 36 órán belül – köteles a jelen szabályzat melléklete szerinti jegyzőkönyv kitöltött és aláírt példányát szkennelve, elektronikus úton megküldeni az ügyvezető részére vagy ennek lehetetlenülése esetén az incidensről más módon tájékoztatást adni.

VI. 5. Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár az érintettek jogaira és szabadságaira nézve, vagy az adatvédelmi hatóság így rendelkezik, az Adatkezelő köteles haladéktalanul tájékoztatni az érintetteket az adatvédelmi incidens bekövetkezéséről. A tájékoztatásnak legalább a következőkre ki kell terjednie:

- a) az adatvédelmi incidens bekövetkezésének időpontja, körülményei;
- b) az incidens jellege (pl. fertőzés, hackertámadás, adathordozó elvesztése, stb. következtében adatok megsemmisülése, elvesztése, illetéktelen személyek számára hozzáférhetővé válása);
- c) annak becslése, hogy incidens milyen következményekkel jár az érintettek jogaira, szabadságaira, milyen súlyos a bekövetkezett sérelem;
- d) a kár vagy sérelem orvoslására vagy elhárítására tett vagy tenni tervezett intézkedések leírása;

VI.6. A VI.5. pont szerinti tájékoztatást tömör, átlátható, érthető formában, világosan és közérthetően megfogalmazva kell megtenni. A tájékoztatás megtehető a jelen szabályzat mellékletét képező jegyzőkönyv megküldésével is. A tájékoztatás díjmentes.

VI.7. Nem kell az érintetteket tájékoztatni az adatvédelmi incidensről a következő esetekben:

- a) az Adatkezelő megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre, és ezeket az intézkedéseket az adatvédelmi incidens által érintett adatok tekintetében alkalmazták, különösen azokat az intézkedéseket – mint például a titkosítás alkalmazása –, amelyek a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetlenné teszik az adatokat;
- b) az Adatkezelő az adatvédelmi incidenst követően olyan további intézkedéseket tett, amelyek biztosítják, hogy az érintett jogaira és szabadságaira jelentett magas kockázat a továbbiakban valószínűsíthetően nem áll fenn;
- c) a tájékoztatás aránytalan erőfeszítést tenne szükségessé. Ilyen esetekben az érintetteket az

Adatkezelő honlapján kiadott közlemény útján kell tájékoztatni.

VI.8. Az incidensről – a jelen szabályzat mellékletét képező jegyzőkönyv használatával - a Nemzeti Adatvédelmi és Információszabadság Hatóságot (NAIH) is értesíteni szükséges. A tájékoztatást, elektronikus úton szükséges megküldeni a NAIH email címére az incidens bekövetkezésétől számított 72 órán belül. A tájékoztatást az ügyvezető teszi meg.

VI.9. Nem szükséges az incidens bejelentése a NAIH-hoz, amennyiben az incidens valószínűsíthetően nem jár kockázattal az érintettek jogaira és szabadságaira nézve.

VI.10. Tekintettel a GDPR vonatkozó rendelkezéseire az Adatkezelő nem köteles adatvédelmi tisztviselő kijelölésére.

VII. Az érintett jogai, kérései teljesítésének szabályai

VII.1. Az érintett jogai az alábbiak:

- tájékoztatáshoz való jog: Az érintett jogosult arra, hogy adatainak kezelésére irányuló tevékenység megkezdését megelőzően tájékoztatást kapjon az adatkezeléssel összefüggő információkról.

- hozzáféréshez való jog: Az érintett jogosult arra, hogy az adatkezelőtől visszajelzést kapjon arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e, és ha ilyen adatkezelés folyamatban van, jogosult arra, hogy a személyes adatokhoz és a releváns információkhoz hozzáférést kapjon (adatkezelés célja, érintett személyes adatok, személyes adatok tárolásának időtartama, stb.)

- helyesbítéshez és törléshez való jog: Az érintett jogosult arra, hogy kérésére az adatkezelő indokolatlan késedelem nélkül helyesbítse a rá vonatkozó pontatlan személyes adatokat. Az érintett jogosult arra, hogy kérésére az adatkezelő indokolatlan késedelem nélkül törölje a rá vonatkozó személyes adatokat, az adatkezelő pedig köteles arra, hogy az érintettre vonatkozó személyes adatokat indokolatlan késedelem nélkül törölje, ha az érintett kifejezett hozzájárulását visszavonta, illetve az adatkezelés célja egyéb okból megszűnt.

- az adatkezelés korlátozásához való jog: Az érintett jogosult arra, hogy kérésére az adatkezelő korlátozza az adatkezelést, ha vitatja a személyes adatok pontosságát (ez esetben a korlátozás arra az időtartamra vonatkozik, amely lehetővé teszi, hogy az adatkezelő ellenőrizze a személyes adatok pontosságát); az adatkezelés jogellenes, és az érintett ellenzi az adatok törlését, és ehelyett kéri azok felhasználásának korlátozását; az adatkezelőnek már nincs szüksége a személyes adatokra adatkezelés céljából, de az érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez.

- személyes adatok helyesbítéséhez, vagy törléséhez, illetve az adatkezelés korlátozásához kapcsolódó értesítési kötelezettség: Az adatkezelő 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.

- adathordozhatósághoz való jog: Az érintett jogosult arra, hogy a rá vonatkozó, általa egy adatkezelő rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja, továbbá jogosult arra, hogy ezeket az adatokat egy másik adatkezelőnek továbbítsa.

- tiltakozáshoz való jog: Az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból bármikor tiltakozzon személyes adatainak a közérdekű vagy közhatalmi jogosítvány gyakorlásának keretében megvalósuló adatkezelése, illetve az adatkezelő, vagy harmadik fél jogos érdekeinek érvényesítéséhez szükséges adatkezelés ellen (a rendelet 6. cikk (1) bekezdésének e) vagy f) pontján alapuló adatkezelés), ideértve az említett rendelkezéseken alapuló profilalkotást is. Ebben az esetben az adatkezelő a személyes adatokat nem kezelheti tovább, kivéve, ha az adatkezelő 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.

- automatizált döntéshozatal alóli mentesség joga: Az érintett jogosult arra, hogy ne terjedjen ki rá az olyan, kizárólag automatizált adatkezelésen – ideértve a profilalkotást is – alapuló döntés hatálya, amely rá nézve joghatással járna vagy őt hasonlóképpen jelentős mértékben érintené.

- panasztételhez és jogorvoslathoz való jog: Az érintett a GDPR 77. cikke alapján jogosult arra, hogy panaszt tegyen a felügyeleti hatóságnál, ha az érintett megítélése szerint a rá vonatkozó személyes adatok kezelése megsérti a GDPR-t. Panasztételhez való jogát az érintett az alábbi elérhetőségeken gyakorolhatja:

Nemzeti Adatvédelmi és Információszabadság Hatóság cím: 1125 Budapest, Szilágyi Erzsébet fasor 22/c Telefon: +36 (1) 391-1400; Fax: +36 (1) 391-1410 www: <http://www.naih.hu> email: ugyfelszolgalat@naih.hu

VII.2. Amennyiben az érintett gyakorolni kívánja a GDPR III. fejezetében meghatározott jogokat, az Adatkezelő késedelem nélkül, de legkésőbb 30 napon belül köteles – széles körben alkalmazott formátum (pl. word, excel) használatával - eleget tenni a jogszerű kérésnek.

VII.3. Amennyiben az Adatkezelő az érintett kérését nem teljesíti, az elutasítás indokát meg kell jelölni, valamint fel kell hívni az érintett figyelmét a bírósági út igénybe vételének lehetőségére.

VII.4. Az e-mailben beérkező kéréseket, valamint a telefonon érkező megkeresések leiratát az ügyvezető részére kell továbbítani.

VII.5. Az Adatkezelő a jelen szabályzat mellékletét képező nyilvántartást vezeti az érintett kéréseiről, azok teljesítéséről, amely legalább a következőket tartalmazza:

- a) Az érintett neve, kapcsolati adatai;
- b) A kérelem tárgya;
- c) A kérelem beérkezésének ideje és teljesítésének ideje;
- d) A kérelem teljesítésének formátuma;
- e) Elutasítás esetén az elutasítás indoka;
- f) Az Adatkezelő megjegyzései.

VII.6. A kérelmet díjmentesen kell teljesíteni. Költségtérítést akkor lehet megállapítani, ha a kérelem teljesítése aránytalan megterhelést jelentene az Adatkezelő számára, illetve az visszaélésszerű.

VII.7. A nyilvánvalóan visszaélésszerű kérelem teljesítése megtagadható.

VIII. Az adatok megismerésére jogosultak köre

VIII.1. A személyes adatokat az Adatkezelő vonatkozó adatkezelési célhoz kapcsolódó hozzáférési jogosultságokkal rendelkező munkavállalói, illetve az Adatkezelő részére szolgáltatási szerződések alapján adatfeldolgozási tevékenységet végző személyek, szervezetek ismerhetik meg, az Adatkezelő által meghatározott terjedelemben és a tevékenységük végzéséhez szükséges mértékben.

VIII.2. Az Adatkezelő által igénybevett, a személyes adatok megismerésére jogosult adatfeldolgozók felsorolása:

1. Cégnév: **NetSoft Informatika Kft.**

Székhely: 1214 Budapest, Erdősor u 16.

Céjegyzekszám: 01-09-369785

Adószám: 12036282-2-43

Képviselő neve: Gáll Kálmán ügyvezető

E-mail: info@netsoft.hu

Weboldal: netsoft.hu

Tevékenység: számlázó program szolgáltatása

2. Cégnév: **Éliás Judit Könyvelő Kft.**

Székhely: 2000 Szentendre, Mókus utca 6.

Céjegyzekszám: 13-09-172301

Adószám: 25049686-2-13

Képviselő neve: Éliás Judit ügyvezető

E-mail: eliasjudit1@gmail.com

Tevékenység: számviteli és bérszámfejtési szolgáltatás

3. Cégnév: **GlobalWeb Consulting Kft.**

Székhely: 1039 Budapest, Juhász Gyula utca 11.

Céjegyzekszám: 01-09-970817

Adószám: 23549221-2-41

Kapcsolattartó: Szőke Lóránd

E-mail: info@globalweboldal.hu

Weboldal: www.globalweboldal.hu

Tevékenység: firstchoice.hu weboldal üzemeltetése

4. Cégnév: **C-Host Kft.**

Székhely: 1115 Budapest, Halmi u. 29.

Céjegyzekszám: 01-09-961790

Adószám: 23358005-2-43

Képviselő: Kárász András

E-mail: info@nethely.hu

Weboldal: www.nethely.hu

Tevékenység: tárhely szolgáltatás

IX. Hatályba léptető és egyéb rendelkezések

IX.1. A jelen szabályzat 2018. május 25. napján lép hatályba.

IX.2. A jelen szabályzatban nem szabályozott kérdésekben a GDPR-t és a hatályos magyar jog szabályait szükséges alkalmazni.

IX.3. A jelen szabályzatot az Adatkezelő köteles szükség szerint, de legalább két évente felülvizsgálni. Az esetleges módosításokkal egységes szerkezetbe foglalt szabályzatot megfelelően nyilvánosságra kell hozni és külön közölni kell mindazokkal, akikre vonatkozóan kötelezettséget állapít meg.

Budapest, 2018. május 25.

Nikolic Mariann
First Choice Hungary Kft.