Multifaktoring Pénzügyi és Szolgáltató Zrt.

Adatvédelmi szabályzat

Hatályos: **2018. október 1. napjától**

Jelen változat a mindenkori módosításokkal egységes szerkezetben rögzíti a szabályzat hatályos szövegét.

Elfogadta a Multifaktoring Pénzügyi és Szolgáltató Zrt. igazgatósága 2018. szeptember 5. napján.

_____

Multifaktoring Zrt.

1. A SZABÁLYZAT CÉLJA

Figyelemmel arra, hogy:

i. A **Multifaktoring Pénzügyi és Szolgáltató Zrt.** (székhelye: H-1027 Budapest, Medve utca 25-29.; a továbbiakban: **Társaság**) tiszteletben tartja az üzleti tevékenységei keretében kezelt személyes adatokat, akár munkavállalók, fogyasztók, szerződéses partnerek, ügyfelek, vagy egyéb érintettek személyes adatairól van szó.

ii. A Társaság az elszámoltathatóság elve alapján felelős a jelen szabályzat, valamint az Adatvédelmi Jogszabályok betartásáért, továbbá képesnek kell lennie a megfelelőség

igazolására is, és köteles folyamatos ellenőrzésekkel biztosítani a megfelelőség fenntarthatóságát.

iii. A Társaság adatkezelésére Adatvédelmi Jogszabályok vonatkoznak, amelyek megsértése miatt jelentős bírságokat és egyéb következményeket vonhat maga után.

A jelen szabályzat célja, hogy

iv. a Társaság az általa kezelt személyes adatok jogszerű felhasználása érdekében meghatározza a személyes adatok kezelése során irányadó adatvédelmi előírásokat, és

v. rögzítse, hogy a Társaság szervezeti egységei, munkavállalói, egyéb tisztviselő hogyan kötelesek eljárni a személyes adatok kezelése során.

2. A SZABÁLYZAT HATÁLYA

2.1. A jelen szabályzat a személyes adatoknak a Társaság általi kezelésére, illetve feldolgozására vonatkozik.

2.2. A szabályzat személyi hatálya kiterjed az Társaság valamennyi szervezeti egységére, a Társasággal munkaviszonyra irányuló jogviszony keretében foglalkoztatott személyekre.

3. ÉRTELMEZŐ RENDELKEZÉSEK

3.1. A jelen szabályzatban az alábbi fogalmak az itt meghatározott jelentéssel bírnak:

3.1.1. **Adatvédelmi Jogszabályok**: a személyes adatok kezelésével, védelmével és felhasználásával kapcsolatos és irányadó jogszabály, ideértve a GDPR-t és a GDPR, annak végrehajtását szolgáló jogszabályt, az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvényt, ezekkel kapcsolatos bármely bírósági vagy hatósági értelmezés, illetve bármely illetékes felügyeleti hatóság (NAIH) által kiadott iránymutatás, útmutató, gyakorlati szabályzat, jóváhagyott etikai kódex, vagy jóváhagyott tanúsítási mechanizmus.

3.1.2. **GDPR**: az **Európai** Parlament és a Tanács (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről („Általános Adatvédelmi Rendelet", angol rövidítése: „GDPR");

3.1.3. **Standard Szerződéses Klauzulák**: Az EU Bizottságának 2010/87. sz. határozata (2010. február 5.) a 95/46/EK európai parlamenti és tanácsi irányelv alapján a személyes adatok harmadik országbeli adatfeldolgozók részére történő továbbítására vonatkozó általános szerződési feltételekről, továbbá az EU Bizottságának 2004/915. sz. határozata 01/497/EK határozat módosításáról a személyes adatoknak harmadik országokba irányuló továbbadására vonatkozó alternatív általános szerződési feltételek bevezetéséről (adatátadási megállapodás, II.csomag).

3.1.4. „**adatkezelő**”, „**adatkezelés**”„**adatfeldolgozó**”, „**adatfeldolgozás**” „**érintett**”, „**személyes adat**”, és „**adatvédelmi incidens**”, és ezek kis kezdőbetűvel írt formái a GDPR-ban meghatározott jelentéssel bírnak.

3.2. A jelen szabályzatot az Adatvédelmi Jogszabályokkal összhangban kell értelmezni.

4. ADATVÉDELMI ALAPELVEK

4.1. A személyes adatok kezelése során a Társaság és munkavállalói kötelesek figyelemmel lenni az alábbi adatvédelmi alapelvekre, és minden egyes adatkezelési műveletet az alábbi legfontosabb adatvédelmi elveknek megfelelően kell végezni. A GDPR 5. cikke szerint a személyes adatok

- kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni („***jogszerűség, tisztességes eljárás és átláthatóság***”);

- gyűjtése csak meghatározott, egyértelmű és jogszerű célból történjen, és azokat ne kezeljék ezekkel a célokkal össze nem egyeztethető módon; a 89. cikk (1) bekezdésének megfelelően nem minősül az eredeti céllal össze nem egyeztethetőnek a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból történő további adatkezelés („***célhoz kötöttség***”);

- az adatkezelés céljai szempontjából megfelelőek és relevánsak kell, hogy legyenek, és a szükségesre kell korlátozódniuk („***adattakarékosság***”);

- pontosnak és szükség esetén naprakésznek kell lenniük; minden észszerű intézkedést meg kell tenni annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul töröljék vagy helyesbítsék („**pontosság**”);

- tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé (ameddig ez a meghatározott cél(ok) eléréséhez szükséges, illetve ameddig ezt a hatályos törvények előírják), („***korlátozott tárolhatóság***”);

- kezelését oly módon kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával 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***”).

4.2. Az adatkezelő felelős a fentiek megfelelésért, továbbá képesnek kell lennie e megfelelés igazolására („***elszámoltathatóság***”).

4.3. A fenti alapelvekre figyelemmel a Társaságnál csak abban az esetben kezelhető személyes adat, ha:

- a megvalósítani kívánt cél másként nem érhető el,

- megfelelő jogalap áll rendelkezésre az adott adatkezelési célhoz,

- az adott adatkezelési célnak megfelelően és ésszerűen került meghatározásra az adatmegőrzési idő tartama,

- az adatkezelésről az érintettet a Társaság tájékoztatta vagy a Társaság az adatkezelésre jogszabály vagy más rendelkezés miatt köteles, és

- az adatkezelés megfelel a fenti 4.1 pontban rögzített egyéb alapelveknek is.

4.4. A Társaság a GDPR által meghatározott jogalapok közül választhat. Ebben az adatkezelés megkezdését és az adatkezelési tájékoztatását megelőzően a Társaság jogászával szükséges konzultálni.

4.5. Abban az esetben, ha valamely adatkezelés jogalapja a Társaság jogos érdekén alapul, a Társaság az adatkezelés megkezdését megelőzően érdekmérlegelési írásbeli teszt elvégzésével köteles meggyőződni arról, hogy a Társaság jogos érdeke alátámasztható-e és mérlegelni szükséges az érintettek érdekeit, jogait. Az érdekmérlegelési teszteket a Társaság nyilvántartja és megőrzi.

4.6. Abban az esetben, ha valamely adatkezelés jogalapja az érintett által adott hozzájárulás, figyelemmel kell lenni arra, a hozzájárulás akkor érvényes, ha 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. Az érintett jogosult hozzájárulását bármikor visszavonni. Amennyiben az adatkezelés egyszerre több célt is szolgál, akkor a hozzájárulást az összes adatkezelési célra vonatkozóan kell megadni.

4.7. Személyes adat csak addig tárolható, ameddig az adatkezelés céljainak eléréséhez szükséges, melyet követően a személyes adatot meg kell semmisíteni vagy anominizálni szükséges.

5. AZ ADATKEZELÉSI TEVÉKENYSÉG NYILVÁNTARTÁSA (GDPR 30. cikk)

5.1. A Társaság, mint adatkezelő a felelősségébe tartozóan végzett adatkezelési tevékenységekről nyilvántartást köteles vezetni. E nyilvántartás a következő információkat tartalmazza:

a) az adatkezelő neve és elérhetősége, valamint – ha van ilyen – a közös adatkezelőnek, az adatkezelő 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) ha lehetséges, a különböző adatkategóriák törlésére előirányzott határidők;
g) ha lehetséges, a GDPR 32. cikk (1) bekezdésében említett technikai és szervezési intézkedések általános leírása.

5.2. Minden adatfeldolgozó köteles nyilvántartást vezetni az adatkezelő nevében végzett adatkezelési tevékenységek minden kategóriájáról, a GDPR 30. cikk (2) bekezdésében előírt tartalommal.

5.3. Az előbbi bekezdések szerinti kötelezettségek nem vonatkoznak a 250 főnél kevesebb személyt foglalkoztató vállalkozásra vagy szervezetre, kivéve, ha az általa végzett adatkezelés az érintettek jogaira és szabadságaira nézve valószínűsíthetően kockázattal jár, ha az adatkezelés nem alkalmi jellegű, vagy ha az adatkezelés kiterjed a személyes adatok különleges kategóriáinak vagy büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó személyes adatoknak a kezelésére.

5.4. A nyilvántartást írásban kell vezetni, ideértve az elektronikus formátumot is.

5.5. Az adatkezelő vagy az adatfeldolgozó megkeresés alapján a felügyeleti hatóság részére rendelkezésére köteles bocsátani a nyilvántartást.

5.6. A fenti kötelezettségek teljesítéséről a Társaság az alábbiak szerint gondoskodik:

5.7. Amennyiben a Társaság adatkezelő:

a) A Társaság az által végzett adatkezelési tevékenységekről adatkezelési célok szerinti bontásban vezeti a nyilvántartást elektronikus úton.
b) A nyilvántartást a Társaság mindenkori adatvédelmi tisztviselője vezeti és gondoskodik annak naprakész voltáról.
c) A nyilvántartást illetéktelen személyek hozzáférésétől, jogosulatlan módosítástól védeni szükséges. A nyilvántartást vezető személy a saját hálózati mappájában vezeti a nyilvántartást, amelyhez kizárólag ő rendelkezik olvasási / szerkesztési jogosultsággal.
d) A nyilvántartásba jogosult betekinteni: az adott szervezeti egység vezetője, adatvédelmi tisztviselő, a Társaság jogásza.
e) A felügyeleti hatóság részére a nyilvántartást csak a Társaság jogászával való előzetes konzultációt követően lehet rendelkezésére bocsátani a Társaság ügyvezetőjének jóváhagyásával. [Az adatvédelmi tisztviselőt tájékoztatni szükséges.]
f) A Társaság köteles gondoskodni arról, hogy az adatfeldolgozóival való együttműködése során az adatfeldolgozó a nyilvántartási kötelezettségének eleget tegyen.

5.8. Amennyiben a Társaság adatfeldolgozó:

a) A Társaság az általa valamely adatkezelő részére végzett adatkezelési tevékenységekről adatkezelők és adatkezelési célok szerinti bontásban vezeti a nyilvántartást elektronikus úton.
b) A nyilvántartást a Társaság mindenkori adatvédelmi tisztviselője vezeti és gondoskodik annak naprakész voltáról.
c) A nyilvántartást illetéktelen személyek hozzáférésétől, jogosulatlan módosítástól védeni szükséges. A nyilvántartást vezető személy a saját hálózati mappájában vezeti a nyilvántartást, amelyhez kizárólag ő rendelkezik olvasási / szerkesztési jogosultsággal.

d) A nyilvántartásba jogosult betekinteni: az adott szervezeti egység vezetője, adatvédelmi tisztviselő, a Társaság jogásza.
e) A felügyeleti hatóság részére a nyilvántartást csak a Társaság jogászával való előzetes konzultációt követően lehet rendelkezésére bocsátani a Társaság ügyvezetőjének jóváhagyásával, amelyről az adatvédelmi tisztviselőt tájékoztatni szükséges.

6. AZ ADATVÉDELMI HATÁSVIZSGÁLAT (GDPR 35. cikk)

6.1. Az adatvédelmi hatásvizsgálat azt a célt szolgálja, hogy a Társaság az egyes adatkezeléseivel kapcsolatosan felmérje az adatvédelmi kockázatokat és az annak mérséklésére szolgáló megoldásokat, intézkedéseket, és a leghatékonyabban eleget tegyen személyes adatok védelmének, így csökkentve a kockázatokat, jogsértésből adódó jogkövetkezményeket, és a Társaság jóhírnevének sérelmét.

6.2. A GDPR 35. cikkében meghatározott esetekben a Társaság köteles adatvédelmi vizsgálatot végezni. Eszerint az Társaság abban az esetben köteles adatvédelmi hatásvizsgálatot végezni, amennyiben új technológiát alkalmaz és ha az adatkezelés valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, Így különösen ide tartozik:

- természetes személyekre vonatkozó egyes személyes jellemzők olyan módszeres és kiterjedt értékelése, amely automatizált adatkezelésen alapulnak, és amely a természetes személy tekintetében joghatással bír (vagy a természetes személyre hasonlóképpen jelentős mértékű hatást gyakorolna);
- személyes adatok különleges kategóriái (pl. egészségügyi adatok vagy a büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó személyes adatok) nagy számban történő kezelése; vagy
- nyilvános helyek nagymértékű, módszeres megfigyelése.

6.3. A hatásvizsgálat kiterjed legalább:

- a tervezett adatkezelési műveletek módszeres leírására és az adatkezelés céljainak ismertetésére, beleértve adott esetben az adatkezelő által érvényesíteni kívánt jogos érdeket;
- az adatkezelés céljaira figyelemmel az adatkezelési műveletek szükségességi és arányossági vizsgálatára;
- az érintett jogait és szabadságait érintő kockázatok vizsgálatára; és
- a kockázatok kezelését célzó intézkedések bemutatására, ideértve a személyes adatok védelmét és az e rendelettel való összhang igazolását szolgáló, az érintettek és más személyek jogait és jogos érdekeit figyelembe vevő garanciákat, biztonsági intézkedéseket és mechanizmusokat.

6.4. Az adatvédelmi hatásvizsgálatot a Társaság a fentieken kívül javasolja elvégezni bármely új folyamat, project, tevékenység megkezdése előtt, amennyiben az feltehetően személyes adatok kezelésével jár a Társaság részéről.

6.5. Az adatvédelmi hatásvizsgálatot a Társaság elektronikus formában, kérdőív (szoftver) keretében végzi. Az adatvédelmi hatásvizsgálati kérdőívet az adott adatkezelési tevékenységért felelős szervezeti egység vezetője, illetve az új technológia bevezetését kezdeményező személy válaszolja meg, és a Társaság ügyvédje ellenőrzi, hagyja jóvá, gondoskodik kockázatok enyhítését szolgáló lépések megtételéről.

6.6. Az adatkezelő az adatvédelmi hatásvizsgálat elvégzésekor az adatvédelmi tisztviselő szakmai tanácsát köteles kikérni.

6.7. A már elvégzett adatvédelmi hatásvizsgálatot a Társaság köteles felülvizsgálni, illetve megismételni, amennyiben az adatkezelésben változás következik be. Ezt az adott adatkezelési tevékenységért felelős szervezeti egység vezetője kezdeményezi.

6.8. Az előbbiektől függetlenül a Társaság évente felülvizsgálja az adatkezelési folyamatait és a hatásvizsgálatok aktuálisak-e.

7. SZERZŐDÉSES PARTNEREK, NEMZETKÖZI ADATTOVÁBBÍTÁS

7.1. Az Adatvédelmi Jogszabályok különbséget tesznek az „adatkezelő" és az „adatfeldolgozó" között. Adatkezelő az a természetes vagy jogi személy, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza. Az adatkezelő határozza meg a személyes adatok kezelésének *céljait* és *eszközeit*, aki irányítást gyakorol az adatkezelési tevékenység felett. Adatfeldolgozó az a természetes vagy jogi személy, aki az adatkezelő nevében személyes adatokat kezel.

7.2. Annak megítélése, hogy a Társaság és a Társasággal szerződő fél valamely adatkezelés tekintetében adatkezelőnek vagy adatfeldolgozónak minősül, a Társaság jogászának hatáskörébe tartozik. A szerződő felek adatvédelmi szempontú minősítése azért fontos, mert az adatkezelőt, illetve az adatfeldolgozót az Adatvédelmi Jogszabályok alapján eltérő kötelezettségek terhelik, amely a felek közötti szerződéskötésre hatással van.

7.3. Abban az esetben, ha a Társaság adatkezelő és egy külső szolgáltatóval kíván szerződést kötni, aki adatfeldolgozónak minősül, akkor

7.3.1. a szolgáltatót a szerződést kötést megelőzően ellenőrizni szükséges adatvédelmi szempontból megfelelő és megbízható működéséről; továbbá

7.3.2. a felek kötelesek adatfeldolgozási szerződést kötni írásban. A szerződésnek az adatfeldolgozó jogait és kötelezettségeit tartalmaznia kell, továbbá mindazon rendelkezéseket, amelyet a vonatkozó Adatvédelmi Jogszabályok, vagy egyéb jogszabályok előírnak. Az adatfeldolgozási szerződést legalább a GDPR 28. cikk (3) bekezdésben foglalt tartalommal szükséges megkötni.

7.4. Az adatfeldolgozó az adatkezelő előzetesen írásban tett eseti vagy általános felhatalmazása nélkül további (al)adatfeldolgozót nem vehet igénybe.

7.5. Abban az esetben, ha Társaság az adatkezelés céljait és eszközeit más adatkezelővel közösen határozza meg, azok közös adatkezelőknek minősülnek. A közös adatkezelők átlátható módon, a közöttük létrejött megállapodásban kötelesek meghatározni kötelezettségeikkel, feladataikkal összefüggő felelősségük megoszlását, a GDPR 26. cikkében foglaltaknak megfelelően.

7.6. Személyes adatok továbbítására minden esetben csak akkor kerülhet sor, ha az vonatkozó Adatvédelmi Jogszabályok, különösen a GDPR rendelkezéseinek megfelel. Ennek megítélése a Társaság jogászának feladatkörébe tartozik, így harmadik országba személyes adat továbbítására a véleményének kikérését követően kerülhet sor.

7.7. A Társaság köteles gondoskodni arról, hogy a kezelésében lévő személyes adatokat csak olyan esetekben továbbíthat harmadik országba (az EGT-n kívülre), ha a GDPR V. fejezetében foglaltak valamelyikének megfelel. Ennek alapján a Társaság különösen akkor továbbíthat személyes adatot harmadik országba, ha az EU Bizottság döntése alapján az megfelelő szintű védelmet biztosít, vagy a felek Standard Szerződéses Klauzulát kötnek, továbbá az EU és az USA közötti Adatvédelmi Pajzsnak (Privacy Shield) a részese, vagy az érintett kifejezetten hozzájárulását adta a tervezett továbbításhoz azt követően, hogy tájékoztatták az adattovábbításból eredő esetleges kockázatokról.

8. AZ ADATKEZELÉS BIZTONSÁGA (GDPR 32. cikk)

8.1. A Társaság a tudomány és 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 megfelelő technikai és szervezési intézkedéseket hajt végre annak érdekében, ideértve, többek között, adott esetben:

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.

8.2. A biztonság megfelelő szintjének meghatározásakor kifejezetten figyelembe kell venni az adatkezelésből eredő olyan kockázatokat, amelyek különösen a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítéséből, elvesztéséből, megváltoztatásából, jogosulatlan nyilvánosságra hozatalából vagy az azokhoz való jogosulatlan hozzáférésből erednek.

8.3. Az adatkezelés biztonsága érdekében meg kell tenni a szükséges technikai és szervezési intézkedéseket mind az informatikai eszközök útján tárolt, mind a hagyományos, papíralapú adathordozókon tárolt adatállományok tekintetében.

8.4. A Társaság az adatkezelés megfelelő biztonságát a vele szerződést kötő adatfeldolgozóktól is elvárja, és a velük való szerződést kötést megelőzően a Társaság meggyőzik arról, hogy az adatfeldolgozó megfelelően biztosítani tudja a Társaság nevében kezelt adatokat.

8.5. Az adatbiztonság garantálásáról a Társaság informatikai (IT) részlege gondoskodik.

8.6. Az adatbiztonságra vonatkozó részletes szabályokat az a Társaság külön utasításokban, illetve szabályzatokban határozhatja meg.

9. ADATVÉDELMI INCIDENSEK KEZELÉSE (GDPR 33. és 34. cikke)

9.1. 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.

9.2. Adott esettől függően a Társaság köteles lehet értesíteni a megfelelő felügyeleti hatóságot (NAIH) a személyes adatokat érintő adatvédelmi incidensekről. Súlyos incidensek esetén az érintettek értesítésére is szükség lehet. A személyes adatokat érintő adatvédelmi incidenseket minden esetben a jelen szabályzatban foglaltaknak megfelelően kell kivizsgálni és kezelni.

9.3. Felelősségi körök adatvédelmi incidenssel kapcsolatosan:

pozíció	**feladat**
Ügyvezetés	Adatvédelmi megfelelőség biztosítása a Társaságnál, végső döntéshozatal.
IT	Felelős az adatvédelmi incidens informatikai szempontú kezeléséért. – Gondoskodik incidens kezelés informatikai szempontú eljárásrendjéről. – Tanácsot ad az adatvédelmi incidens minősítéséhez az informatika szempontok alapján. – Együttműködik Jogásszal, szükség szerint egyéb munkavállalókkal, ügyvezetéssel az incidens értékelésében. – Tanácsot ad a kockázatok enyhítését, jövőbeli hasonló események bekövetkezésének elkerülését illetően.
ADATVÉDELMI TISZTVISELŐ	– Együttműködik az adatvédelmi incidens minősítésében és értékelésében. – Tanácsot ad a kockázatok enyhítését,
pozíció	**feladat**

	jövőbeli hasonló események bekövetkezésének elkerülését érintően, amennyiben az nem az IT feladatát érinti. – Megteszi a szükséges értesítéseket.
JOGÁSZ (ÜGYVÉD)	– Tanácsot ad az adatvédelmi incidens minősítéséhez az Adatvédelmi Jogszabályok alapján. – IT-val, szükség szerint egyéb munkavállalók bevonásával értékeli az incidensről szóló bejelentést. – Tanácsot ad a kockázatok enyhítését, jövőbeli hasonló események bekövetkezésének elkerülését érintően, amennyiben az nem az IT feladatát érinti. – Előkészíti a NAIH, illetve érintettek részére szóló értesítést. – Oktatja a Társaság munkavállalóit az adatvédelmi incidensek bejelentésével és kezelésével összefüggő tudnivalókról.
ÉRINTETT ÜZLETI EGYSÉG	– Együttműködik Jogásszal, IT-val szükség szerint egyéb munkavállalókkal, ügyvezetéssel az incidens értékelésében, és a kockázatok enyhítését, jövőbeli hasonló események bekövetkezésének elkerülését érintően.
MUNKAVÁLLALÓK	– gyanús esemény bejelentése – együttműködés az esemény kivizsgálásában, – oktatáson való részvétel.

9.4. Bejelentés:

9.4.1. A Társaság bármely munkavállalója adatvédelmi incidens gyanúja esetén haladéktalanul köteles az adatvedelmifelelos@multifaktoring.hu email címre bejelentést tenni. A bejelentést tartalmazó e-mail tárgyában fel kell tüntetni az „bejelentés, sürgős és bizalmas". A bejelentés formanyomtatványát a jelen szabályzat 1.számú melléklete tartalmazza.

9.4.2. A bejelentés kézhez vevője a bejelentés beérkezését követően haladéktalanul e-mailben vagy telefonon értesíti az ügyvezetést az incidens-bejelentésről.

9.4.3. A bejelentést bizalmasan kell kezelni.

9.5. Kivizsgálás, értékelés:

9.5.1. Az ügyvezetés (akadályoztatásuk esetén az általuk kijelölt munkavállalók) értesítésüket követően haladéktalanul kötelesek vizsgálatot kezdeményezni az IT-nál és Jogásznál, és lefolytatni a vizsgálatot annak megállapításra, hogy történt-e adatvédelmi incidens, illetve szükséges-e bejelentést tenni a NAIH-nak. Továbbá mérlegelni kell, hogy az incidensről tájékoztatni kell-e az érintetteket.

9.5.2. Az incidens bekövetkeztétől számított legfeljebb 72 órán belül az ügyvezetésnek a jelen szabályzat 1. számú mellékletében található incidens bejelentési és értékelési formanyomtatvány minta alapján rögzíteni kell az incidens kivizsgálása során megállapított tényeket. Amennyiben az ügyvezetés rögzíti, hogy indokolt az incidens bejelentése a NAIH-nak, az adatvédelmi tisztviselő vagy jogász köteles a NAIH incidens bejelentésre szolgáló online felületén az incidenst az ott meghatározott szempontok alapján bejelenteni.

9.6. Intézkedések megtétele:

9.6.1. Az adatvédelmi incidenst az adatkezelő indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, bejelenti a NAIH-nak, kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Ha a bejelentés nem történik meg 72 órán belül, mellékelni kell hozzá a késedelem igazolására szolgáló indokokat is.

9.6.2. Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az adatkezelő indokolatlan késedelem nélkül tájékoztatja az érintettet az adatvédelmi incidensről. Az érintettet nem kell tájékoztatni, ha a következő feltételek bármelyike teljesül:

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 értelmezhetetlenné 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 valósul meg;

c) a tájékoztatás aránytalan erőfeszítést tenne szükségessé. Ilyen esetekben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, vagy olyan hasonló intézkedést kell hozni, amely biztosítja az érintettek hasonlóan hatékony tájékoztatását. Ebben az esetben az a Társaság közleményt ad ki belső és/vagy külső honlapján, vagy közvetlenül felveszi a kapcsolatot az érintettekkel (email, telefon, sms).

9.6.3. Adatvédelmi incidens esetén az adatvédelmi tisztviselő köteles a belső nyilvántartásba venni az incidenst, és az ehhez kapcsolódó tényeket, annak hatásait és az orvoslásra tett intézkedéseket. A nyilvántartást jogosulatlan hozzáféréstől védeni kell.

9.7. Audit, ellenőrzés

9.7.1. A Társaság ügyvezetése 1 (egy) hónapon belül ellenőrzi, hogy a megelőzést szolgáló intézkedéseket az arra kijelölt személyek illetve szervezeti egységek vezetői miként hajtották végre.

9.7.2. Az IT gondoskodik az informatikai rendszerek biztonságáról, és rendszeres felülvizsgálatról.

10. AZ ÉRINTETTEK JOGAI (GDPR 12-22.cikk)

10.1. A személyes adatokat az érintett vonatkozó jogaival összhangban kell kezelni, amelyek a GDPR értelmében (a megfelelő mértékben) korlátozás nélkül a következőket jelentik:

- a személyes adatokhoz való hozzáférés jogát;
- az adatkezelés elleni tiltakozás jogát (többek között olyan esetekben, ahol a személyes adatok kezelése közvetlen reklámcélú megkeresés céljából történik);
- az érintetthez kapcsolódó személyes adatok törlésének jogát;
- az adatkezelés korlátozásához való jogot;
- az adathordozhatósághoz való jogot;
- az automatizált döntéshozatal, például a profilalkotás elleni tiltakozás jogát;
- a pontatlan vagy hiányos adatok helyesbítésének vagy kiegészítésének jogát; valamint
- a törvénysértések által okozott károk utáni kártérítés igénylésének jogát.

10.2. A Társaság, mint adatkezelő megfelelő intézkedéseket hoz annak érdekében, hogy az érintett részére a személyes adatok kezelésére vonatkozó minden egyes tájékoztatást tömör, átlátható, érthető és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazva nyújtsa. 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.

10.3. A Társaság az érintett jogai gyakorlására irányuló kérelmének a teljesítését nem tagadhatja meg, kivéve, ha bizonyítja, hogy az érintettet nem áll módjában azonosítani, vagy azt az Adatvédelmi Jogszabály lehetővé teszi.

10.4. A Társaság indokolatlan késedelem nélkül, de mindenféleképpen a kérelem beérkezésétől számított egy hónapon belül tájékoztatja az érintettet a 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 az adatkezelő 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.

10.5. Ha a Társaság 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 valamely felügyeleti hatóságnál, és élhet bírósági jogorvoslati jogával.

10.6. Az információkat és tájékoztatást és intézkedést díjmentesen kell biztosítani. Ha az érintett kérelme egyértelműen megalapozatlan vagy – különösen ismétlődő jellege miatt – túlzó, az adatkezelő, figyelemmel a kért információ vagy tájékoztatás nyújtásával vagy a kért intézkedés meghozatalával járó adminisztratív költségekre:

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

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

10.7. Az érintetti jogok gyakorlására vonatkozó kérelmeket a Társaság mindenkori hivatalos elérhetőségein lehet benyújtatni, és azt haladéktalanul továbbítani szükséges a Társaság jogászának (ügyvédjének).

10.8. A kérelem elbírálása a Társaság jogászának (ügyvédjének) hatáskörébe tartozik.

10.9. A kérelem teljesítésében, végrehajtásban, az ahhoz szükséges információk rendelkezésre bocsátásában a Társaság IT részlege, illetve a kérelemmel érintett szervezeti egysége köteles együttműködni.

11. FELELŐSSÉG, ADATVÉDELMI IRÁNYÍTÁS-SZERVEZÉS

11.1. A Társaság elkötelezett a személyes adatok megfelelő kezelése iránt, és úgy véli, hogy a Társaság sikeres működése szempontjából létfontosságú, hogy az általunk tárolt személyes adatokat törvényesen, a jelen Szabályzatban rögzített elvekkel összhangban kezeljük.

11.2. Ügyvezetés: A jelen szabályzatban foglaltak érvényesítéséért és végrehajtásának ellenőrzéséért a Társaság ügyvezetése felel, és negyedévente beszámol a Társaság tulajdonosai felé a Társaságot érintő jelentősebb adatvédelmi ügyekről, kérdésekről.

11.3. Munkavállalók és vezetőik: A Társaság felelős gondoskodni a Társaság szabályzatainak és eljárásainak hiánytalan betartásáról minden esetben, a jelen szabályzatot is beleértve. A Társaság HR osztálya köteles gondoskodni arról, hogy a Társaság munkavállalói és a részlegek beosztottjai megkapják a szükséges útmutatást, forrásokat és oktatást ahhoz, hogy a jelen szabályzatnak megfelelően végezzék munkájukat. A munkavállalók kötelesek együttműködni, oktatásban résztvenni, és a szabályzatban írtakat betartani.

11.4. Adatvédelmi tisztviselő: Az adatvédelmi tisztviselő a GDPR által előírt, jogszabályon alapuló szerepkör. Amennyiben azt a GDPR kötelezően előírja, a Társaság gondoskodik

adatvédelmi tisztviselő kinevezéséről és biztosítja független, befolyásmentes működését az Adatvédelmi Jogszabályoknak megfelelően.

11.5. Jogász: A Társaság jogásza fontos szerepet tölt be az adatvédelem támogatásában. Így különösen tanácsot ad az Adatvédelmi Jogszabályok alkalmazásában, adatkezelési tájékoztatók elkészítésében, szabályzatok véleményezésében, adatfeldolgozókkal, és egyéb szerződő felekkel való szerződések elkészítésében, adatvédelmi hatásvizsgálat értékelésében, továbbá együttműködik a Társaság szervezeti egységeivel.

11.6. IT: A Társaság IT részlegének vezetője gondoskodik az információ biztonság, adatvédelmi biztonság garantálásáról, incidensek IT szempontú kezeléséről és a kapcsolódó szabályzatok elkészítéséről

12. A SZABÁLYZAT MÓDOSÍTÁSA, FELÜLVIZSGÁLAT

12.1. A Szabályzatot időről-időre, szükség szerint, de legalább évente május 31. napjáig felül kell vizsgálni, és szükség szerint a módosítását kezdeményezni. A felülvizsgálatért a Társaság mindenkori adatvédelmi tisztviselője felelős.

12.2. A módosított szabályzatot a Társaság helyben szokásos módon közzéteszi, és amennyiben szükséges gondoskodik a Társaság munkavállalóinak időközi képzéséről, tréningjéről.

1. számú melléklet

INCIDENS BEJELENTÉSI ÉS KIVIZSGÁLÁSI FORMANYOMTATVÁNY
(minta)

Multifaktoring Zrt.

1. A BEJELENTÉS

A válaszadó neve:.....

Kitöltés dátuma:.....

	KÉRDÉS	VÁLASZ
1.	Kérjük, írja le, hogy mi történt (az esemény).	
2.	Mikor történt?	
3.	Mikor lett rá figyelmes?	
4.	Milyen adatot, személyes adatot érinthet az esemény?	
5.	Az esemény különleges adatot is érinthet (pl. egészségügyi adat)?	
6.	Nagyságrendileg mennyi személyes adatot érinthet a fenti esemény?	
7.	A Társaság üzleti információit, titkait érintheti az esemény?	
8.	Hogyan érintheti az esemény az adatot?	
9.	Hány személyt érinthet az esemény?	

10.	Meg tudja nevezni őket? Kik?	
11.	Ön szerint milyen sérelem érheti a fenti személyeket az esemény	
	következtében? (Pl. fizikai biztonság, pénzügyi veszteség, jó hírnév, emberi méltóság stb.). Lehet az eseménynek szélesebb körben kedvezőtlen, nyilvánosság előtt hatása?	
12.	A fenti eseménnyel kapcsolatban van bármilyen irat, információ a birtokában, ami be tud mutatni vagy át tud adni a Társaságnak?	
13.	Kérjük, írja le ide, amit még el szeretne mondani a fentiekkel kapcsolatban.	

2. AZ ÉRTÉKELÉS ÉS INTÉZKEDÉSEK

Az értékelő neve:.....

Az értékelés kelte:.....

	KÉRDÉS	**VÁLASZ**
1.	Adatvédelmi incidensnek minősül a fenti esemény? Mik lehetnek a fenti adatvédelmi incidens következményei, kockázatok?	
2.	Valószínűsíthető, hogy a fenti esemény az érintett jogaira és szabadságaira kockázatot jelent?	

3.	Mi a kockázat mértéke és miért? (alacsony / közepes / magas)	
4.	Milyen intézkedéseket kell megtenni, amelyek biztosítják, hogy az érintett jogaira és szabadságaira jelentett magas kockázat a továbbiakban valószínűsíthetően nem valósul meg?	
5.	Kinek és milyen lépéseket szükséges megtenni a kockázat csökkentése, elhárítása érdekében?	
6.	Kinek és milyen lépéseket szükséges megtenni, hogy a jövőben a fentihez hasonló esemény / adatvédelmi incidens ne következhessen be?	
7.	Szükséges értesíteni valamely hatóságot (NAIH, rendőrség)?	
8.	Szükséges értesíteni az érintetteket a fenti eseményről? Ha igen, ki és milyen módon teszi meg az értesítést?	

* * *