

BRÜSSZELI MAGYAR HÁZ
NONPROFIT KORLÁTOLT FELELŐSSÉGŰ TÁRSASÁG

Iktatószám: ÜV/10 - 19 /2024.


19/2024. (X.31.) Ügyvezetői utasítás

Tárgy: a Brüsszeli Magyar Ház Nonprofit Korlátolt Felelősségű Társaság Adatvédelmi és Adatbiztonsági Szabályzata

1. A Brüsszeli Magyar Ház Nonprofit Korlátolt Felelősségű Társaság **Adatvédelmi és Adatbiztonsági Szabályzatát** jelen Ügyvezetői utasítás mellékletében foglaltak szerint határozom meg.
2. Jelen ügyvezetői utasítás az aláírás napján lép hatályba és annak módosításáig, illetve visszavonásáig érvényes.

Budapest, 2024. október 31.



Glázer Tamás 
ügyvezető

Kapják:

- 1.) Irattár (eredeti példány)
- 2.) Koordinációs Igazgatóság (elektronikus példány)

Brüsszeli Magyar Ház Nonprofit Korlátolt Felelősségű Társaság

ADATVÉDELMI ÉS ADATBIZTONSÁGI SZABÁLYZAT

Tartalom

I. ÁLTALÁNOS RENDELKEZÉSEK.....	6
1. A Társaság, mint Adatkezelő adatai.....	6
4. A Szabályzat célja.....	7
5. A Szabályzat hatálya.....	8
6. Fogalmak	8
II. AZ ADATKEZELÉS JOGSZERŰSÉGÉNEK BIZTOSÍTÁSA.....	11
1. Az adatkezelés elvei	11
2. Az adatkezelés jogalapjai	12
III. ADATBIZTONSÁGI INTÉZKEDÉSEK	14
1. Adatbiztonsági intézkedések	14
IV. SPECIÁLIS ADATKEZELÉSI SZABÁLYOK.....	15
1. A munkavállalók adatainak kezelésére vonatkozó speciális szabályok.....	15
2. Az Adatkezelő szerződéses partnereire vonatkozó speciális szabályok	16
3. Az elektronikus megfigyelőrendszerre vonatkozó speciális szabályok	16
4. Elektronikus beléptető rendszer alkalmazására vonatkozó speciális szabályok	16
V. BEÉPÍTETT ADATVÉDELEM, ADATVÉDELMI HATÁSVIZSGÁLAT ELVÉGZÉSE.....	16
VI. AZ ADATVÉDELMI INCIDENSEK KEZELÉSÉNEK SZABÁLYAI.....	17
1. Az adatvédelmi incidens fogalma	17
2. Adatvédelmi incidensek kezelése, orvoslása.....	17
3. Adatvédelmi incidensek nyilvántartása	18
4. Az adatvédelmi incidens értékelése	18
5. A Felügyeleti Hatóság tájékoztatása az adatvédelmi incidensről:	19
6. Az érintettek tájékoztatása	20
VII. AZ ÉRINTETTI JOGGYAKORLÁSSAL KAPCSOLATOS INTÉZKEDÉSEK.....	20
1. Intézkedések az Érintett kérelme alapján	20
VIII. AZ ELLENŐRZÉS RENDSZERE /BELSŐ ADATVÉDELMI AUDIT	21
IX. NYILVÁNTARTÁSOK, AZ ELSZÁMOLTATHATÓSÁG ELVÉNEK BIZTOSÍTÁSA	21
(2) Ügyvezető.....	22
(3) Rendezvény és Programigazgató.....	23
(4) Koordinációs Igazgató.....	23
(5) Jogtanácsos.....	23
(6) Titkársági referens	23
(7) Az Adatvédelmi tisztviselő	24
XV. ZÁRÓ RENDELKEZÉSEK	31
1. A Szabályzat megállapítása és módosítása.....	31
2. Intézkedések a Szabályzat megismertetése vonatkozásában	31

I. ÁLTALÁNOS RENDELKEZÉSEK

1. A Társaság, mint Adatkezelő adatai

Név: **Brüsszeli Magyar Ház Nonprofit Kft.**
Székhelye: 1013 Budapest, Ybl Miklós tér 6.
Telefonszáma: +36 30 322 3908
E-mail címe: info@maisondehongrie-bruxelles.hu
Az adatvédelmi tisztviselő
elérhetősége: e-mail: dpo@maisondehongrie-bruxelles.hu
(a továbbiakban: **Társaság** vagy **Adatkezelő**)

Az Európai Parlament és a Tanács (EU) 2016/679 Rendeletének - (2016. április 27.) 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 szóló (General Data Protection Regulation, azaz Általános Adatvédelmi Rendelet, *a továbbiakban: **GDPR** vagy **Rendelet***)-, valamint az információs jogról és az információszabadságról szóló 2011. évi CXII. törvény (*a továbbiakban: **Infotv.***) való megfelelés céljából a Társaság saját, a Rendelet hatálya alá tartozó adatkezelését a jelen Szabályzatban meghatározott szabályok szerint végzi.

A Társaság Adatvédelmi és Adatbiztonsági Szabályzatát és a hatályban lévő Adatkezelési tájékoztatóit a honlapján vagy egyéb, a Rendelet és az Infotv. előírásainak megfelelő módon teszi elérhetővé az Érintettek számára. A jelen Szabályzat célja, hogy az Érintetteket az adatkezelés megkezdése előtt és annak folyamán is egyértelműen és részletesen tájékoztassa az adataik kezelésével kapcsolatos minden tényről, így különösen az adatkezelés céljáról és jogalapjáról, az adatkezelésre és az adatfeldolgozásra jogosult személyéről, az adatkezelés időtartamáról, arról, ha az Érintett személyes adatait az Adatkezelő az Infotv. 5. § (5) bekezdése alapján kezeli, illetve arról, hogy kik ismerhetik meg az adatokat. A tájékoztatásnak ki kell terjednie az Érintett adatkezeléssel kapcsolatos jogaira és jogorvoslati lehetőségeire is. Az egyes adatkezelési műveletekre vonatkozó Adatkezelési Tájékoztatók elérhetőségéről az Érintetteket tájékoztatni kell.

2. Az adatvédelem szervezete

A Társaság Ügyvezetője felelős a személyes adatok védelméért és a Társaság tevékenységre vonatkozó közérdekű adatok nyilvánosságára vonatkozó törvényi előírások érvényesítéséért. A Társaság Ügyvezetője az adatvédelemmel és az információszabadsággal kapcsolatos feladatát a közvetlen irányítása alatt álló Adatvédelmi tisztviselő útján látja el (*a továbbiakban: **Adatvédelmi tisztviselő***).

3. Az Adatvédelmi tisztviselő

- (1) Tekintettel a tényre, mely szerint a Társaság a Rendelet 37. cikkének (1) bekezdés a) pontja szerinti közfeladatot ellátó szervnek minősül, Adatvédelmi tisztviselő kijelöléséről köteles gondoskodni.
- (2) Adatvédelmi tisztviselőnek olyan természetes személy jelölhető ki, aki felsőfokú informatikai vagy jogi végzettséggel rendelkezik, ismeri az európai és hazai adatvédelemmel kapcsolatos főbb

szabályokat, rendelkezik alapvető informatikai ismeretekkel, illetve az adatvédelem területén szerzett legalább 3 éves gyakorlattal.

(3) Nem lehet adatvédelmi tisztviselő, aki a Társaságnál az adatkezelési tevékenység céljainak, kereteinek, eszközeinek meghatározásáról dönt, különösen az Ügyvezető, az IT vezető, a pénzügyi vezető, a HR vezető, valamint a belső ellenőr.

(4) Az adatvédelmi tisztviselőt az Ügyvezető jelöli ki.

(5) A Társaság, mint Adatkezelő biztosítani köteles, hogy az Adatvédelmi tisztviselő a személyes adatok védelmével kapcsolatos összes ügybe megfelelő módon és időben be tudjon kapcsolódni. Ezzel párhuzamosan a Társaság biztosítja az Adatvédelmi tisztviselő számára azokat a forrásokat, amelyek a feladatai végrehajtásához, a személyes adatokhoz és az adatkezelési műveletekhez való hozzáféréshez, valamint az Adatvédelmi tisztviselő szakértői ismereteinek fenntartásához, elmélyítéséhez, bővítéséhez szükségesek.

(6) Az Adatvédelmi tisztviselő a feladatai ellátása során független, utasítást senkitől nem fogad el, közvetlenül az Adatkezelő Ügyvezetőjének tartozik felelősséggel.

(7) Az Érintettek a személyes adataik kezeléséhez és a Rendelet szerinti jogaik gyakorlásához kapcsolódó valamennyi kérdésben az Adatvédelmi tisztviselőhöz jogosultak fordulni.

(8) Az Adatvédelmi tisztviselő feladatait az adatkezelési műveletekhez kapcsolódó kockázatok mindenkori és megfelelő figyelembevételével, az adatkezelés jellegére, hatókörére, körülményére és céljára is tekintettel végzi.

(9) Az Adatvédelmi tisztviselő - a jogszabályban és e Szabályzatban meghatározott - adatvédelmi feladatai ellátásával összefüggésben nem bocsátható el és szankcióval nem sújtható.

(10) Az Adatvédelmi tisztviselőt feladatai teljesítésével kapcsolatban uniós vagy tagállami jogban meghatározott titoktartási kötelezettség vagy az adatok bizalmas kezelésére vonatkozó kötelezettség köti.

4. A Szabályzat célja

A Társaság az általa kezelt személyes adatokat minden esetben a hatályos magyar és európai jogszabályoknak, valamint adatkezelési elveknek megfelelően kezeli, és egyben biztosítja azokat a garanciális feltételeket, amelyek a biztonságos adatkezeléshez szükségesek. A Társaság annak érdekében, hogy adatkezelési tevékenysége megfeleljen a GDPR és az Infotv. rendelkezéseinek, a jelen Szabályzatban határozza meg azokat az irányelveket, szabályokat és felelősségi rendeket, továbbá rendszerezíti azokat az intézkedéseket, eljárásrendet, amelyek biztosítják, hogy a Társaság adatkezelése megfeleljen a jelen pontban hivatkozott jogszabályok rendelkezéseinek.

A Szabályzat további célja, hogy a Társaság által végzett adatkezelés működésének jogszerű rendjét, valamint az adatvédelem alkotmányos elveinek érvényesülését, továbbá az információs önrendelkezési jognak és az adatbiztonság követelményeinek érvényesülését biztosítsa.

Jelen Szabályzat célja, hogy biztosítsa a Társaság adatkezelése során a személyes adatok védelméhez fűződő jogok érvényesülését, és a jogosulatlan felhasználás megakadályozását; meghatározza azon technikai és szervezési intézkedéseket, melyek biztosítják az adatbiztonságot a személyes adatok kezelése során; illetve rögzítse a Társaságnál vezetett, személyes adatokat tartalmazó nyilvántartások vezetésének szabályait.

5. A Szabályzat hatálya

- (1) E Szabályzat hatálya a természetes személyek adatainak a Társaság által történő kezelésére vonatkozik. Jelen Szabályzat alkalmazása során az egyéni vállalkozókat, jogi személyek természetes személy képviselőit szintén természetes személyeknek kell tekinteni. A Szabályzat hatálya nem terjed ki az olyan személyes adatkezelésre, amely jogi személyekre vonatkozik, beleértve a jogi személy nevét és formáját, valamint a jogi személy elérhetőségére vonatkozó adatokat.
- (2) A Szabályzat tárgyi hatálya kiterjed - az adatkezelési módszertől függetlenül - a Társaságnál folyó valamennyi ügyintézési és ügykezelési eljárásra, munkafolyamatra, amennyiben természetes személy adatát is érinti.
- (3) A Jelen Szabályzat személyi hatálya az alábbi személyekre terjed ki: Társaság irányítása alatt eljáró, személyes adatokhoz hozzáféréssel rendelkező személyek (a munkavégzésre irányuló jogviszony jellegétől függetlenül, közreműködők); valamint azok természetes személyek, akik személyes adatait a jelen Szabályzat hatálya alá tartozó adatkezelések tartalmazzák (érintettek).
- (4) A Szabályzat hatálya nem terjed ki a közérdekű adatok elektronikus közzétételének és a közérdekű adatigénylések teljesítésének rendjére, melyről külön Szabályzat rendelkezik.
- (5) Az adatfeldolgozásra az adatkezelés szabályait kell alkalmazni.

6. Fogalmak

- (1) A jelen Szabályzatban és a Társaság adatkezelési tevékenységei és kommunikációja során használt fogalmak elsősorban a GDPR (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 irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet) – a továbbiakban Rendelet) alapján kerültek meghatározásra az alábbiak szerint:
 - (a) *Érintett*: minden olyan természetes személy, aki valamely személyes adata alapján közvetlenül, vagy közvetve azonosíthatóvá válik, és akivel kapcsolatban Adatkezelő adatkezelést végez. Érintettnek minősül pl.: ügyfél, törvényes képviselő, munkavállaló
 - (b) *személyes adat*: az Érintettre vonatkozó bármely adat vagy információ, mely az Érintettel kapcsolatba hozható, vagy az Érintettet azonosíthatóvá teszi (pl.: név, telefonszám, online azonosító, helymeghatározó adat, arckép, hang, stb....) [Rendelet 4. cikk 1.] A személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az Érintettel – az Adatkezelő által birtokolt információk és technikai feltételek segítségével – helyreállítható
 - (c) *adatvédelem*: a személyes adatok jogszerű kezelését, az érintett személyek védelmét biztosító alapelvek, szabályok, eljárások, adatkezelési eszközök és módszerek összessége
 - (d) *adatbiztonság*: az adatok jogosulatlan megszerzése, módosítása és megsemmisítése elleni műszaki és szervezési megoldások rendszere
 - (e) *adatkezelés*: bármely, személyes adatokon Adatkezelő vagy Adatfeldolgozó által végzett tevékenység. Az adatkezelés történhet automatizált vagy nem automatizált módon (pl.: gyűjtés, rögzítés, rendszerezés, tárolás, felhasználás, továbbítás, megsemmisítés) [Rendelet 4. cikk. 2.]

(f) *adatfeldolgozó*: az a természetes vagy jogi személy, szerv, mely az Adatkezelő nevében és felhatalmazása alapján adatokat kezel. Jelen adatvédelmi Szabályzat rendelkezései Adatfeldolgozóra is vonatkoznak

(g) *közös adatkezelő*: az az adatkezelő, aki vagy amely – törvényben vagy az Európai Unió kötelező jogi aktusában meghatározott keretek között – az adatkezelés céljait és eszközeit egy vagy több másik adatkezelővel közösen határozza meg, az adatkezelésre vonatkozó döntéseket egy vagy több másik adatkezelővel közösen hozza meg és hajtja végre vagy hajtatja végre az adatfeldolgozóval

(h) *harmadik fél*: az a természetes vagy jogi személy, mely nem azonos az Érintettel, az Adatkezelővel, az Adatfeldolgozóval, a közös adatkezelővel, illetve az Adatfeldolgozó és Adatkezelő közvetlen irányítása alatt álló, adatok kezelésére felhatalmazott személlyel. [Rendelet 4. cikk 10.]

(i) *kiskorú*: az a természetes személy, aki a tizennyolcadik életévét nem töltötte be. [Ptk. 2:10. §]

(j) *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 megfelelően az alkalmazandó adatvédelmi szabályoknak [Rendelet 4. cikk. 9.]

(k) *egészségügyi személyes adat*: egy természetes személy testi vagy szellemi 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; [Infotv. 3.§ (3) c)] ezek közé tartoznak az érintett egészségi állapotára vonatkozó olyan adatok, amelyek információt hordoznak az érintett múltbeli, jelenlegi vagy jövőbeli testi vagy pszichikai egészségi állapotáról [Rendelet 4. cikk].

(l) *különleges személyes adat*: a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a természetes személyek egyedi azonosítását célzó genetikai és biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok [Rendelet 9. cikk (1) bek]

(m) *biometrikus adat*: a természetes személy fizikai, fiziológiai vagy viselkedési jellemzőire vonatkozó olyan, sajátos technikai eljárásokkal nyert személyes adat, mely lehetővé tesz vagy megerősíti a természetes személy egyedi azonosítását, mint például az arckép vagy a daktiloszkópiai adat (pl.: ujjlenyomat)

(n) *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.

(o) *az érintett hozzájárulása*: az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy a megerősített félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez [Rendelet 4. cikk]. Különleges adatok esetében szükséges az írásos forma.

(p) *adattvédelmi 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 [Rendelet 4. cikk]

(q) *érdekmérlegelési teszt*: a jogos érdek, mint adatkezelési jogalap meglétét alátámasztó, az Adatkezelő jogos érdekeinek érvényesítéséhez szükséges, az Adatkezelő és az érintett jogos érdekeinek összehasonlításán alapuló teszt, melynek eredménye meghatározza, hogy az Adatkezelő jogos érdeke alkalmazható-e az adatkezelés jogalapjaként.

(r) *adatkezelési nyilvántartás*: adatkezelő és - ha van ilyen - az adatkezelő képviselője a felelősségébe tartozóan végzett adatkezelési tevékenységekről szóló nyilvántartás, mely a következő információkat tartalmazza: a) az adatkezelő neve és elérhetősége, valamint - ha van ilyen - a közös adatkezelőnek, az adatkezelő képviselőjének és az adattvédelmi 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 49. cikk (1) bekezdésének második albekezdés szerinti továbbítás esetében a megfelelő garanciák leírása; f) ha lehetséges, a különböző adatkezelési kategóriák törlésére előírt határidők; g) ha lehetséges, a 32. cikk bekezdésében említett technikai és szervezési intézkedések általános leírása [Rendelet 30. cikk (1) bekezdés]

(s) *adatkezelésért felelős személy*: az adattvédelmi tisztviselő mely az adatkezeléssel kapcsolatos feladatokat (pl.: nyilvántartások vezetése) ellátja

(t) *adattvédelmi hatásvizsgálat*: olyan vizsgálat, amelyet az adatkezelésért felelős személy köteles elvégezni, amennyiben valamely tervezett adatkezelés – figyelemmel annak jellegére, hatókörére, körülményeire és céljaira, ideértve különösen az új technológiák alkalmazásának esetét – valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, és amelynek célja annak megállapítása, hogy a tervezett adatkezelés a személyes adatok védelmét hogyan érinti. Az adattvédelmi hatásvizsgálat egy olyan eljárás, amelynek során az adatkezelő a tervezett adatkezelési műveletet vagy műveleteket áttekinti, megvizsgálja az adatkezelés érintettekre gyakorolt esetleges hatását, felméri annak kockázatait, a kockázatok kezelésének módját, és mindezt megfelelően dokumentálja. Adattvédelmi tisztviselő közreműködik a hatásvizsgálat elvégzése során

(u) *adattvédelmi tisztviselő*: a Társaság szervezetében működő, a Rendelet 39. cikkében meghatározott feladatokat a jelen Szabályzatában foglaltak szerint ellátó, a Társasággal megbízási jogviszonyban álló személy

(v) *adattovábbítás külföldre*: személyes adatok továbbítása EGT-n (Európai Gazdasági Térség: az Európai Unió országai, valamint Izland, Norvégia és Liechtenstein) kívüli, harmadik országban adatkezelési tevékenységet folytató adatkezelőhöz

(w) *információszabadság*: a közérdekű, valamint közérdekből nyilvános adatok megismeréséhez és terjesztéséhez fűződő alapvető jog, mely elősegíti a közhatalom gyakorlásának demokratikus kontrollját és a közintézmények átláthatóságát (transzparencia)

(x) *közérdekű adat*: az állami/önkormányzati feladatot, illetve egyéb közfeladatot ellátó szerv kezelésében lévő és tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben

keletkezett, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől (így különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre, annak eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat).

(y) *közérdekből nyilvános adat*: a közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli. (pl. a hitelezői érdekek védelme, valamint a piaci forgalom biztonsága érdekében az adatok széles körét minősíti közérdekből nyilvánosnak az ingatlan-nyilvántartásról szóló törvény, a cégtörvény, valamint a számviteli törvény)

(z) *nyilvánosságra hozatal*: az adat bárki számára történő hozzáférhetővé tétele

(aa) *adattörlés*: az adat felismerhetlenné tétele oly módon, hogy a helyreállítása többé nem lehetséges

(bb) *adatkezelés korlátozása*: a tárolt adat zárolása az adat további kezelésének korlátozása céljából történő megjelölés útján

(cc) *profilalkotás*: a személyes adat bármely olyan automatizált módon történő kezelése, amely az érintett személyes jellemzőinek, különösen munkahelyi teljesítményéhez, gazdasági helyzetéhez, egészségi állapotához, személyes preferenciáihoz vagy érdeklődéséhez, megbízhatóságához, viselkedéséhez, tartózkodási helyéhez vagy mozgásához kapcsolódó jellemzőinek értékelése, elemzése vagy előrejelzésére irányul

(dd) *álnevesítés*: személyes adat olyan módon történő kezelése, amely a személyes adattól elkülönítve tárolt további információ felhasználása nélkül megállapíthatatlanná teszi, hogy a személyes adat mely érintetthez vonatkozik, valamint műszaki és szervezési intézkedések megtételével biztosítja, hogy azt az azonosított vagy azonosítható természetes személyhez ne lehessen kapcsolni

(ee) *üzleti titok*: a gazdasági tevékenységhez kapcsolódó titkos, ennél fogva vagyoni értékkel bíró olyan tény, tájékoztatás, egyéb adat és az azokból készült összeállítás, amelynek a titokban tartása érdekében a titok jogosultja az adott helyzetben általában elvárható magatartást tanúsítja.

II. AZ ADATKEZELÉS JOGSZERŰSÉGÉNEK BIZTOSÍTÁSA

1. Az adatkezelés elvei

A Szabályzat hatálya alá tartozó személyek tevékenységük során kötelesek a Társaság, mint adatkezelő kezelésében lévő adatokat a mindenkori jogszabályoknak megfelelően kezelni, a következő alapelvek mindenkori szem előtt tartásával:

a.) *jogszerűség*: A személyes adatok kezelése során az Adatkezelőnek, az Adatfeldolgozónak, illetve közvetlen irányításuk alatt álló, adatkezelésre felhatalmazott személyeknek meg kell felelniük a mindenkori hatályos európai uniós és hazai jogszabályoknak.

b.) *tisztességes eljárás*: Az adatkezelés során Adatkezelőnek a jogszabályokat és alapelveket tiszteletben tartva, korrekt módon kell eljárnia.

- c.) *átláthatóság*: A személyes adatok kezelését az Érintettek számára átlátható, megismerhető módon kell elvégezni.
- d.) *célhoz kötöttség*: A személyes adatok bármilyen kezelése kizárólag meghatározott, egyértelmű és jogszerű célból történhet. Az adatkezelési tájékoztatók tartalmazzák az Adatkezelő által kezelt adatok adatkezelési célját az adatok felvételétől kezdődően azok megsemmisítéséig. [Rendelet 5. cikk. (1) bekezdés b)] Csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen, s a cél elérésére alkalmas. A személyes adat csak a cél megvalósulásáig kezelhető.
- e.) *adattakarékosság*: Az adatkezelést – a célhoz kötöttség elve alapján – kizárólag a releváns és szükséges adatokra kell korlátozni. [Rendelet 5. cikk. (1) bekezdés c)]
- f.) *arányosság*: Adatkezelő a természetes személyek információs önrendelkezéshez való jogát kizárólag egy másik jog érdekében, a szükséges mértékben korlátozhatja. Az arányosság elvének megvalósulását a konkrét esetekben pontosan dokumentálni kell az adatkezelés jogszerűségének alátámasztására. [Rendelet 6. cikk. (1) bekezdés f)]
- g.) *pontosság*: Az adatkezelés során – az adatkezelés elveit figyelembe véve – törekedni kell a pontatlan adatok helyesbítésére vagy törlésére. [Rendelet 5. cikk. (1) bekezdés d)]
- h.) *elszámoltathatóság*: Adatkezelő felelős a jogszabályokban és jelen Szabályzatban foglaltak betartásáért és betartatásáért. Adatkezelő úgy alakítja ki adatkezelési folyamatait, hogy az adatkezelési elveknek és szabályoknak való megfelelése igazolható legyen. [Rendelet 5. cikk. (2) bekezdés]
- i.) *privacy-by-design*: Adatkezelő adatkezelési folyamatai kialakítása során figyelemmel van az adatbiztonság és adatkezelés elveire, melyek megvalósulását a folyamatba épített elemekkel kívánja biztosítani. A Társaság a nyilvántartási rendszerének felépítése, a jogosultságok meghatározása, és egyéb szervezeti intézkedések útján gondoskodik arról, hogy a személyes adatokat tartalmazó iratokat csak azok a munkavállalók, illetve egyéb, a Társaság érdekkörében eljáró személyek ismerhessék meg, akiknek ere a munkakörül, feladatok ellátása érdekében szükséges. Az adatállományok kezelésére, azok biztonságok őrzésére, a hozzáférési jogokra, adatok, dokumentumok felhasználására a Társaságra vonatkozó hatályos szabályzatok, utasítások az irányadóak.
- j.) *privacy by default*: Az Adatkezelő alapvető, „alapértelmezett” (angolul: by default) hozzáállása az kell, hogy legyen, hogy minden körülmények között figyelembe veszi az adatvédelmi szempontokat és ezeknek megfelelően járnak el az adatkezelési műveletek során.

2. Az adatkezelés jogalapjai

A Rendelet 6. cikke alapján jogszerűnek minősül az adatkezelés, amennyiben a következő esetek valamelyike fennáll:

- a.) az Érintett – előzetes tájékoztatás alapján – hozzájárulását adta személyes adatainak kezeléséhez [Rendelet 6. cikk (1) bekezdés a) pont)]
- b.) az adatkezelés egy olyan szerződés előkészítéséhez vagy teljesítéséhez szükséges, melyben az Érintett az egyik fél [Rendelet 6. cikk (1) bekezdés b) pont)]
- c.) az adatkezelést jogszabály teszi kötelezővé Adatkezelő számára [Rendelet 6. cikk (1) bekezdés c) pont)]
- d.) az adatkezelés az Érintett, vagy másik személy létfontosságú érdekeinek védelme érdekében

szükséges [Rendelet 6. cikk (1) bekezdés d) pont])

e.) az adatkezelés közérdekű, vagy az Adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges [Rendelet 6. cikk

(1) bekezdés e) pont))

f.) az adatkezelés az Adatkezelő, vagy harmadik fél jogos érdekének védelme vagy érvényesítése érdekében szükséges [Rendelet 6. cikk (1) bekezdés f) pont]]

Jogi kötelezettség teljesítése, kötelező adatkezelés esetén a kezelendő adatok fajtáit, az adatkezelés célját és feltételeit, az adatok megismerhetőségét, az adatkezelés időtartamát, valamint az adatkezelő személyét az adatkezelést elrendelő törvény, illetve önkormányzati rendelet határozza meg.

18 éven aluli kiskorú érintett személy esetén törvényes képviselője jogosult nyilatkozatot tenni (pl.: adatkezelési hozzájáruló nyilatkozat).

Ha az érintett cselekvőképтелensége folytán vagy más elháríthatatlan okból nem képes hozzájárulását megadni, akkor a saját vagy más személy létfontosságú érdekeinek védelméhez, valamint a személyes életét, testi épségét vagy javait fenyegető közvetlen veszély elhárításához vagy megelőzéséhez szükséges mértékben a hozzájárulás akadályainak fennállása alatt az érintett személyes adatai kezelhetők.

Adatkezelő tevékenysége során a rá ruházott közhatalmi jogosítvány gyakorlásában végzett feladatok végrehajtása érdekében kezel adatokat. Ezen jogalap esetén az adatkezelés tekintetében annak szükségesnek kell lennie. Ez a jogalap tartalmazhat a Rendeletben foglalt szabályok alkalmazását kiigazító rendelkezéseket, ideértve az adatkezelő általi adatkezelés jogszerűségére irányadó általános feltételeket, az adatkezelés tárgyát képező adatok típusát, az érintetteket, azokat a jogalanyokat, amelyekkel a személyes adatok közölhetők, illetve az ilyen adatközlés céljait, az adatkezelés céljára vonatkozó korlátozásokat, az adattárolás időtartamát és az adatkezelési műveleteket, valamint egyéb adatkezelési eljárásokat, így a törvényes és tisztességes adatkezelés biztosításához szükséges intézkedéseket is, ideértve a Rendelet IX. fejezetében meghatározott egyéb konkrét adatkezelési helyzetekre vonatkozóan. Az uniós vagy tagállami jognak közérdekű célt kell szolgálnia, és arányosnak kell lennie az elérni kívánt jogszerű céllal.

A kötelező adatkezelés keretében kezelt személyes adatokat – ha a törvény eltérően nem rendelkezik – a Központi Statisztikai Hivatal statisztikai célból, egyedi azonosításra alkalmatlan módon átveheti és a törvényben meghatározott módon kezelheti. Ezen adatok kizárólag statisztikai célra kezelhetők. A személyes adatok statisztikai célú kezelését egyebekben külön jogszabály határozza meg.

III. ADATBIZTONSÁGI INTÉZKEDÉSEK

A Társaság elkötelezett amellett, hogy szigorúan védje az Érintett személyes adatait, tiszteletben tartsa az Érintett ilyen adatok felhasználására vonatkozó döntését, és gondosan védelmezze, nehogy elveszenek, azokkal visszaéljenek, azokhoz jogosulatlanul hozzáférjenek, vagy azokat hozzáférhetővé tegyék, megváltoztassák vagy megsemmisítsék, továbbá törekszik arra, hogy az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válást megelőzze.

1. Adatbiztonsági intézkedések

- (1) A Társaság valamennyi adatkezelése vonatkozásában a személyes adatok biztonsága érdekében megteszi azokat a technikai és szervezési intézkedéseket, kialakítja az eljárási szabályokat, amelyek a Rendelet és az Infotv. előírásainak betartásához szükségesek. Társaság az adatbiztonsági szabályokat elsősorban a beépített adatvédelem elvét figyelembe véve, a Rendelet 25. cikk és 32. cikkben foglaltakat szem előtt tartva alakítja ki.
- (2) Az Adatkezelő az adatokat megfelelő intézkedésekkel védi a véletlen vagy jogellenes megsemmisítés, elvesztés, megváltoztatás, sérülés, jogosulatlan nyilvánosságra hozatal vagy az azokhoz való jogosulatlan hozzáférés ellen.
- (3) A Társaság a személyes adatokat bizalmas adatként minősíti és kezeli. A munkavállalókkal a személyes adatok kezelésére vonatkozóan titoktartási kötelezettséget ír elő. A személyes adatokhoz való hozzáférést a Társaság jogosultsági szintek megadásával korlátozza.
- (4) A Társaság az informatikai rendszereket tűzfallal védi, és vírusvédelemmel látja el.
- (5) A Társaság az elektronikus adatfeldolgozást, nyilvántartást úgy végzi, hogy az megfeleljen az adatbiztonság követelményeinek. A Társaság biztosítja, hogy az adatokhoz csak célhoz kötötten, ellenőrzött körülmények között és csak azon személyek férjenek hozzá, akiknek a feladataik ellátása érdekében erre szükségük van.
- (6) A személyes adatok kezelése és feldolgozása során az Adatkezelő és az Adatfeldolgozó biztosítja:
 - a) a jogosulatlan adatbevitel megakadályozását;
 - b) a jogosulatlan személyek általi, adatátviteli berendezés segítségével történő használat megakadályozását;
 - c) annak ellenőrizhetőségét és megállapíthatóságát, hogy a személyes adatokat adatátviteli berendezés alkalmazásával mely szerveknek továbbították vagy továbbíthatják;
 - d) annak ellenőrizhetőségét és megállapíthatóságát, hogy mely személyes adatokat, mikor és ki vette nyilvántartásba;
 - e) azt, hogy a kezelés és a feldolgozás során fellépő hibákról jelentés készüljön;
 - f) szükség szerint elvégzi a személyes adatok álnevesítését és titkosítását;
 - g) vizsgálja a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítását, integritását, rendelkezésre állását és ellenálló képességét;
 - h) vizsgálja az arra való képességet fizikai vagy műszaki incidens esetén, hogy a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását kellő időben vissza lehessen állítani;

- i) kialakítja az informatikai biztonság keretében az adatkezelés biztonságának garantálására hozott technikai és szervezési intézkedések hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárást;
- j) a biztonság megfelelő szintjének meghatározására kockázatelemzést végez a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítéséből, elvesztéséből, megváltoztatásából, jogosulatlan nyilvánosságra hozatalából vagy az azokhoz való jogosulatlan hozzáférésekből felmerülő kockázatok azonosítására és azok súlyának az általuk okozható kár meghatározására.

- (7) A Társaság a személyes adatok védelme érdekében gondoskodik az elektronikus úton folytatott bejövő és kimenő kommunikáció ellenőrzéséről.
- (8) A folyamatban levő munkavégzés, feldolgozás alatt levő iratokhoz csak az illetékes munkatársak férhetnek hozzá, a személyzeti, a bér- és munkaügyi és egyéb személyes adatokat tartalmazó iratokat biztonságosan elzárva kell tartani.
- (9) Biztosítani kell az adatok és az azokat hordozó eszközök, iratok megfelelő fizikai védelmét.
- (10) A Társaság az adatbiztonság feltételeinek érvényesítése érdekében gondoskodik az érintett munkatársak megfelelő tájékoztatásáról.
- (11) Adatkezelőnek az adatok biztonságát szolgáló intézkedések meghatározása során tekintettel kell lenni a mindennapi használatba beépült és általánosan elterjedt technika mindenkori fejlettségére. Több lehetséges adatkezelési megoldás közül azt kell választani, amely a személyes adatok magasabb szintű védelmét biztosítja, kivéve, ha az aránytalan nehézséget jelentene Adatkezelőnek vagy munkavállalóinak.

IV. SPECIÁLIS ADATKEZELÉSI SZABÁLYOK

1. A munkavállalók adatainak kezelésére vonatkozó speciális szabályok

- (1) Az Adatkezelő köteles munkavállalót tájékoztatni az adatai kezeléséről.
- (2) A munkavállalótól csak olyan nyilatkozat megtétele vagy adat közlése kérhető, amely személyhez fűződő jogát nem sérti és a munkaviszony létesítése, teljesítése vagy megszűnése szempontjából lényeges.
- (3) A munkavállalóval szemben csak olyan alkalmassági vizsgálat alkalmazható, amelyet munkaviszonyra vonatkozó szabály ír elő, vagy amely a munkaviszonyra vonatkozó szabályban meghatározott jog gyakorlása, kötelezettség teljesítése érdekében szükséges.
- (4) A munkaviszonyból származó kötelezettségek teljesítése céljából az Adatkezelő a munkavállaló személyes adatait adatfeldolgozó számára átadhatja. Erről a munkavállalót előzetesen tájékoztatja.
- (5) A munkavállalók nem jogosultak a munkavégzéshez használt számítástechnikai eszközökön munkaviszonnyal nem összefüggő adatot tárolni, azt magáncélra használni. E kötelezettség megszegése esetén, a munkavégzés ellenőrzése során Adatkezelő nem tekinthet be a munkavállalónak a munkavégzéshez használt számítástechnikai eszközön tárolt, nem a munkaviszonnyal összefüggő adataiba.

2. Az Adatkezelő szerződéses partnereire vonatkozó speciális szabályok

- (1) Adatkezelő szerződéses partnereivel való kapcsolata során kezeli a partnerek kapcsolattartói és képviselői adatait. Adatkezelő a szerződésben tájékoztatja az adatkezelésről üzleti partnereit. Adatkezelő lehetőség szerint szerződésben rögzíti, hogy partnerei tájékoztassák érintett munkavállalóikat az adatkezelés tényéről.
- (2) Amennyiben a megkötött szerződés tekintetében közzétételi kötelezettség áll fent, a Szerződéses partner a szerződés megkötésekor hozzájárul a közzétételhez. Adatkezelő tájékoztatja Partneret, hogy a közzététel megtagadása esetén a jogszabályi keretek között Partnerrel polgári jogi szerződés megkötésére nincs lehetősége.

3. Az elektronikus megfigyelőrendszerre vonatkozó speciális szabályok

- (1) Adatkezelő a jól látható helyen, jól olvashatóan köteles figyelemfelhívó jelzést elhelyezni, melyben tájékoztatja érintetteket az alábbiakról:
 - a.) arról a tényről, hogy az adott területen elektronikus megfigyelőrendszer működik
 - b.) az elektronikus megfigyelőrendszer által folytatott megfigyelés, valamint a rendszer által rögzített, személyes adatokat tartalmazó kép- és hangfelvétele készítésének, tárolásának céljáról, az adatkezelés jogalapjáról, az adatkezelés időtartamáról, az adatkezelő és – amennyiben van – adatfeldolgozó személyéről, az érintettek alapvető jogairól
- (2) Nem alkalmazható elektronikus megfigyelőrendszer olyan helyen, ahol a megfigyelés az emberi méltóságot sértheti, így különösen öltözőben, próbafülkében, mosdóban, kórházi szobában és szociális intézmény lakóhelységében.
- (3) Adatkezelő az elektronikus megfigyelőrendszer alkalmazásával kapcsolatos szabályokról külön szabályzatot alkot (Kameraszabályzat).

4. Elektronikus beléptető rendszer alkalmazására vonatkozó speciális szabályok

- (1) Elektronikus beléptető rendszer akkor alkalmazható, ha a jogszabály vagy a terület használatára jogosult rendelkezése szerint a védett területre csak az arra jogosultak léphetnek be.
- (2) Az elektronikus beléptető rendszer működtetéséhez felhasznált személyes adatok kezelése során biztosítani kell a Rendelet szerinti adatvédelmi jogok érvényesülését, valamint tájékoztatást kell elhelyezni az adatkezelő személyéről és az adatok kezelésének módjáról.

V. BEÉPÍTETT ADATVÉDELEM, ADATVÉDELMI HATÁSVIZSGÁLAT ELVÉGZÉSE

- (1) A Társaságnak az új adatkezelés megkezdése előtt (különösen új adatkezelési technológiák alkalmazása esetén), ha annak jellege, hatóköre, körülményei és céljai, valószínűsíthetően magas kockázattal járnak a természetes személyek jogaira és szabadságaira nézve, az adatkezelést

megelőzően hatásvizsgálatot végez arra vonatkozóan, hogy a tervezett adatkezelési műveletek a személyes adatok védelmét hogyan érintik.

- (2) A Társaság Ügyvezetője hatásvizsgálat elvégzésekor kikéri az Adatvédelmi tisztviselő tanácsát.
- (3) A hatásvizsgálatot az alábbi esetekben kell elvégeznie a Társaságnak:
 - a) természetes személyekre vonatkozó egyes személyes jellemzők olyan módszeres és kiterjedt értékelése, amely automatizált adatkezelésen - ideértve a profilalkotást is - alapul, és amelyre a természetes személy tekintetében joghatással bíró vagy a természetes személyt hasonlóképpen jelentős mértékben érintő döntések épülnek;
 - b) személyes adatok különleges kategóriáinak; vagy
 - c) nyilvános helyek nagymértékű, módszeres megfigyelése.
- (4) A hatásvizsgálat kiterjed az alábbiakra:
 - a) a tervezett adatkezelési műveletek módszeres leírására és az adatkezelés céljainak ismertetésére, beleértve adott esetben az adatkezelő által érvényesíteni kívánt jogos érdeket is;
 - b) az adatkezelés céljaira, figyelemmel az adatkezelési műveletek szükségességi és arányossági vizsgálatára;
 - c) az Érintett jogait és szabadságait érintő kockázatok vizsgálatára;
 - d) a kockázatok kezelését célzó intézkedések bemutatására, ideértve a személyes adatok védelmét és a Rendelettel való összhang igazolását szolgáló, az érintettek és más személyek jogait és jogos érdekeit figyelembe vevő garanciákat, biztonsági intézkedéseket és mechanizmusokat.
- (5) A vizsgálat alapján az Adatvédelmi tisztviselő megállapítja, hogy megtörtént-e az adatkezelési műveletek hatásainak értékelése. Amennyiben az adatvédelmi hatásvizsgálat megállapította, hogy az adatkezelés az Adatkezelő által a kockázat mérséklése céljából tett intézkedések hiányában valószínűsíthetően magas kockázattal jár, a személyes adatok kezelését megelőzően az Adatvédelmi tisztviselő konzultációt folytat a Felügyeleti Hatósággal.

VI. AZ ADATVÉDELMI INCIDENSEK KEZELÉSÉNEK SZABÁLYAI

1. Az adatvédelmi incidens fogalma

- (1) Az 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
- (2) A leggyakoribb jelentett incidensek lehetnek például: a laptop, usb kulcs, vagy mobiltelefon elvesztése, személyes adatok nem biztonságos tárolása (pl. szemetesbe dobott bérszámfejtési dokumentumok); az adatok nem biztonságos továbbítása, a személyes adatokat tartalmazó dokumentumok illetéktelen másolása, továbbítása, szerver elleni támadások, honlap feltörése.

2. Adatvédelmi incidensek kezelése, orvoslása

- (1) Az Adatvédelmi incidensek megelőzése, kezelése, a vonatkozó jogi előírások betartása a Társaság Ügyvezetőjének feladata.

- (2) Az informatikai rendszereken naplózni kell a hozzáféréseket és hozzáférési kísérleteket és ezeket folyamatosan elemezni kell.
- (3) Amennyiben a Társaság ellenőrzésre jogosult munkavállalói a feladataik ellátása során adatvédelmi incidenst észlelnek, haladéktalanul értesíteniük kell a Társaság Ügyvezetőjét.
- (4) A Társaság munkavállalói kötelesek jelenteni a Társaság Ügyvezetőjének, vagy a munkáltatói jogok gyakorlójának, ha adatvédelmi incidenst, vagy arra utaló eseményt észlelnek. Bármely munkavállaló, megbízott, illetve adatfeldolgozó észleli az adatvédelmi incidenst, köteles haladéktalanul, de legfeljebb 24 órán belül bejelenteni (jelzés) a Titkársági referensnek az adatvédelmi tisztviselőnek is. Amennyiben az adatvédelmi incidens jelzése szóban (telefonon vagy személyesen) történik, azt a szóbeli közlést követő legfeljebb 24 órán belül írásban is meg kell erősíteni. Ilyen esetben a szóbeli közlés időpontját külön fel kell tüntetni.
- (5) Az adatvédelmi incidens bejelenthető a Társaság központi e-mail címén, telefonszámán, amelyen a munkavállalók, szerződő partnerek, az Érintettek jelenteni tudják az alapul szolgáló eseményeket, biztonsági gyengeségeket.

3. Adatvédelmi incidensek nyilvántartása

- (1) Adatvédelmi incidens felmerülése, vagy bejelentése esetén a Társaság Ügyvezetője az Adatvédelmi tisztviselő útján az érintett szervezeti egység vezetőjével, illetve elektronikus adatok érintettsége esetén az IT szolgáltatást biztosító szervezet segítségével - haladéktalanul megvizsgálja a bejelentést, ennek során azonosítani kell az incidenst, el kell dönteni, hogy valódi incidensről, vagy téves riasztásról van-e szó. Meg kell vizsgálni és meg kell állapítani:
 - a) az incidens bekövetkezésének időpontját és helyét;
 - b) az incidens leírását, körülményeit, hatásait;
 - c) az incidens során kompromittálódott adatok körét, számosságát;
 - d) a kompromittálódott adatokkal érintett személyek körét;
 - e) az incidens elhárítása érdekében tett intézkedések leírását;
 - f) a kár megelőzése, elhárítása, csökkentése érdekében tett intézkedések leírását.
- (2) Adatvédelmi incidens bekövetkezése esetén az érintett rendszereket, személyeket, adatokat be kell határolni és el kell különíteni. Gondoskodni kell az incidens bekövetkezését alátámasztó bizonyítékok begyűjtéséről és azok megőrzéséről. Ezt követően lehet megkezdeni a károk helyreállítását, a jogszerű működés visszaállítását.
- (3) A nyilvántartásban szereplő adatvédelmi incidensekre vonatkozó adatokat 5 évig meg kell őrizni.

4. Az adatvédelmi incidens értékelése

- (1) A vizsgálat során az adatvédelmi incidenst értékelni kell. A Társaság az alábbi feltételek fennállása esetén minősíti kockázatosnak az adatvédelmi incidenst:
 - az incidensben érintett adatok között találhatóak-e a személyes adatok különleges kategóriába eső adatok,
 - az incidensben érintett adatok száma meghaladja-e a 100 darabot,
 - az incidensben érintett természetes személyek között találhatóak-e kiskorú természetes személyek

- az incidensben érintett természetes személyek száma meghaladja-e a 100 főt,
- az incidensben érintett személyes adatok alkalmasak az érintettel történő közvetlen kapcsolatfelvételre,
- az incidensben érintett adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges
- a személyes adatok alkalmasak az érintett természetes személy személyazonosságának ellopására vagy a személyazonosságával való visszaélésre
- az incidensben érintett személyes adatok alkalmasak arra, hogy a pénzügyi veszteséget okozzanak az Érintetteknek.

(2) A Társaság valószínűsíthetően alacsony kockázatúnak minősíti az incidenst, ha a kockázatoság minősítés feltételei közül legalább egy fennáll, illetve valószínűsíthetően magas kockázatúnak minősíti az adatvédelmi incidenst, ha a kockázatoság minősítés feltételei közül legalább kettő fennáll és a Társaság nem képes annak bizonyítására, hogy az érintett személyes adatokat olyan fizikai és/vagy informatikai védelemmel látta el, amely védelem az incidens bekövetkezése óta nem sérült.

5. A Felügyeleti Hatóság tájékoztatása az adatvédelmi incidensről:

(1) Az Adatvédelmi tisztviselő – a részére történő megküldéstől számított 24 órán belül – a vizsgálat eredményéről tájékoztatja Ügyvezetőt. Az Ügyvezető 24 órán belül dönt a Rendelet 33. cikke szerinti adatvédelmi felügyeleti hatósági bejelentés szükségességéről.

(2) A Rendelet 33. cikkének (1) bekezdése alapján az adatvédelmi incidenst az Adatkezelő indokolatlan késedelem nélkül, de ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, bejelenti az illetékes Felügyeleti Hatóság számára, kivéve, ha az adatvédelmi incidens nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Ha a bejelentés megtétele kötelező, és az nem történik meg 72 órán belül, úgy az Adatkezelő a bejelentés megtételekor mellékeli a késedelem igazolására szolgáló indokokat is.

(3) A (2) bekezdés szerinti bejelentésben az Adatkezelő:

- a) ismerteti az adatvédelmi incidens jellegét, valamint, ha ez a körülményeket tekintve lehetséges, az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát;
- b) közli az Adatvédelmi tisztviselő, valamint a tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;
- c) ismerteti az adatvédelmi incidensből eredő, valószínűsíthető következményeket;
- d) ismerteti az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve az adatvédelmi incidensből származó esetleges hátrányos következmények enyhítését célzó intézkedéseket.

(4) Amennyiben nem lehetséges az információkat egyidejűleg közölni, azok további indokolatlan késedelem nélkül a későbbiekben is közölhetők (ún. szakaszos bejelentés).

6. Az érintettek tájékoztatása

(1) Amennyiben a vizsgálat alapján az incidens vélhetően magas kockázattal jár a természetes személyek jogaira és szabadságára, úgy az érintetteket haladéktalanul értesíteni kell. Az értesítést – az Ügyvezető utasítása alapján, az adatvédelmi tisztviselő javaslatait figyelembe véve – a Titkársági referens adja ki a Koordinációs Igazgató bevonásával.

(2) Az Érintetteket írásban elektronikusan vagy postai úton kell tájékoztatni, mely kizárólag akkor mellőzhető, ha az Érintett elérhetősége ismeretlen. Ilyen jellegű Érintettek esetén a Társaság jogosult a tájékoztatást weboldalán történő közzététellel teljesíteni. A tájékoztatást minden esetben úgy kell teljesíteni, hogy tartalma és ténye bizonyítható legyen.

VII. AZ ÉRINTETTI JOGGYAKORLÁSSAL KAPCSOLATOS INTÉZKEDÉSEK

1. Intézkedések az Érintett kérelme alapján

(1) A kérelmeket beérkezésüket követően dokumentálni kell, mely tartalmazza a kérelem beérkezésének dátumát.

(2) A Társaság, mint Adatkezelő indokolatlan késedelem nélkül, de mindenféleképpen a kérelem beérkezésétől számított egy hónapon belül tájékoztatja az Érintettet a jogai gyakorlására irányuló kérelme nyomán hozott intézkedésekről.

(3) Szükség esetén, figyelembe véve a kérelem összetettségét és a kérelmek számát, ez a határidő további két hónappal meghosszabbítható. A határidő meghosszabbításáról az Adatkezelő - az Adatvédelmi tisztviselő útján - a késedelem okainak megjelölésével a kérelem kézhezvételétől számított egy hónapon belül tájékoztatja az Érintettet.

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

(5) Ha az Adatkezelő 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.

A Társaság, mint Adatkezelő a Rendelet 13. és 14. cikk szerinti információkat és az Érintett jogairól szóló tájékoztatást (Rendelt 15-22. és 34. cikk) és intézkedést díjmentesen biztosítja. 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: észszerű díjat számíthat fel, vagy megtagadhatja a kérelem alapján történő intézkedést.

Ha az Adatkezelőnek megalapozott kétségei vannak a kérelmet benyújtó természetes személy kilétével kapcsolatban, további, az Érintett személyazonosságának megerősítéséhez szükséges információk nyújtását kérheti - Adatkezelő mindaddig jogosult az intézkedés megtételétől tartózkodni, míg megalapozott kétségei hitelt érdemlően és megnyugtatóan rendezésre kerülnek.

- (6) Az Adatkezelő nyilvántartást vezet az adatvédelmi tárgyú kérelmekről és beadványokról, mely a következőket tartalmazza:
- adatvédelmi kérelmet előterjesztő személy neve és kapcsolattartási adatai,
 - kérelem tárgya,
 - beadvány beérkezésének dátuma és módja,
 - megválaszolás dátuma és módja,
 - a kérelem nyomán hozott intézkedések.
- (7) Az Adatkezelő külön szabályzatot hoz a közérdekű adatok igénylésével kapcsolatos eljárási szabályokról.

VIII. AZ ELLENŐRZÉS RENDSZERE /BELSŐ ADATVÉDELMI AUDIT

- (1) A Társaság Ügyvezetője az Adatvédelmi tisztviselő által folyamatba építve vizsgálja az Infotv. és a GDPR végrehajtásával összefüggő kötelezettségek teljesítését. A belső adatvédelmi audit célja, hogy adatvédelmi tisztviselő meggyőződjön róla, hogy Adatkezelő eleget tesz-e a jogszabályban és jelen Szabályzatban foglalt adatkezelési elveknek és rendelkezéseknek. A vizsgálat eredményéről az Adatvédelmi tisztviselő évente legalább egy alkalommal átfogó jelentést készít a Társaság Ügyvezetője részére.
- (2) Az Adatvédelmi tisztviselő évente ellenőrzi, hogy a Társaság szervezeti egységei:
- eleget tesznek-e az elektronikusan kötelezően közzéteendő adatok közzétételére vonatkozó kötelezettségüknek;
 - eleget tesznek-e a közérdekű adatigénylésekkel kapcsolatos kötelezettségüknek;
 - eleget tesznek-e az adatleltárak vezetésével kapcsolatos kötelezettségüknek;
 - eleget tesznek-e az adatvédelmi incidensekkel kapcsolatos kötelezettségüknek;
 - eleget tesznek-e a munkavállalók, ügyfelek, partnerek személyes adatai védelmével kapcsolatos kötelezettségüknek.
- (3) Az ellenőrzésről szükség szerint jegyzőkönyvet készít és hiányosság esetén 15 napon belül javaslatot tesz a Társaság Ügyvezetője részére, hogy 15 napos határidővel hívja fel az érintett szervezeti egység vezetőjét a hiányosság orvoslására.
- (4) Adatvédelmi tisztviselő rendkívüli ellenőrzést is lefolytathat, ha adatvédelmi szempontból az indokolt, különösen, ha a személyes adatkezeléssel érintettek száma jelentős.
- (5) Amennyiben az audit visszásságokat tár fel az adatkezelés terén, adatvédelmi tisztviselő javaslatot tesz a szükséges intézkedésekre a visszásságok megszüntetése érdekében.

IX. NYILVÁNTARTÁSOK, AZ ELSZÁMOLTATHATÓSÁG ELVÉNEK BIZTOSÍTÁSA

- (1) A Társaság szervezeti egységei és projektjei - az Adatvédelmi tisztviselő közreműködésével és irányításával - a Rendelet 30. cikke alapján az adatvédelemmel kapcsolatos jogszabályi előírásoknak való megfelelés bizonyítása érdekében írásbeli elektronikus nyilvántartást vezetnek a hatáskörük alapján végzett adatkezelési tevékenységek fajtáiról. A Társaság a Felügyeleti Hatósággal való

együttműködés keretében ezeket a nyilvántartásokat kérésre hozzáférhetővé teszi az érintett adatkezelési műveletek ellenőrzése érdekében.

- (2) A vezetett nyilvántartások:
 - a) Érintetti hozzájárulások nyilvántartása,
 - b) adattovábbítási nyilvántartás,
 - c) adatszolgáltatási nyilvántartás,
 - d) általános adatleltár,
 - e) Érintetti jogok biztosításának nyilvántartása,
 - f) adatkezelési tájékoztatók nyilvántartása,
 - g) adatvédelmi incidens nyilvántartás.
- (3) Az Adatkezelési Nyilvántartás célja a Társaság adatkezelési tevékenységei átláthatóságának biztosítása.
- (4) Az Adatkezelési Nyilvántartást – elsősorban a Koordinációs Igazgatótól kapott adatok alapján – az Adatvédelmi tisztviselő vezeti.
- (5) Az Adatvédelmi Nyilvántartás minden adatkezelés esetén tartalmazza a következőket:
 - a) adatkezelés célja,
 - b) az érintettek kategóriáinak, valamint a személyes adatok kategóriái,
 - c) adatok forrását,
 - 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 Rendelet 49. cikk (1) bekezdésének második albekezdés szerinti továbbítás esetében a megfelelő garanciák leírása,
 - f) a különböző adatkategóriák törlésére előírányzott határidők – ha lehetséges a meghatározásuk,
 - g) technikai és szervezési intézkedések általános leírását,
 - h) adatfeldolgozó neve és elérhetősége.
- (6) Adatvédelmi tisztviselő a felügyeleti hatóság megkeresésére adatot szolgáltat az Adatkezelési Nyilvántartásból.

X. AZ ADATKEZELÉSSSEL KAPCSOLATOS FELADATOK ÉS HATÁSKÖRÖK

- (1) A Társaság munkavállalói, megbízottai, illetőleg egyes szervezeti egységei a jelen Szabályzatban meghatározottak szerint vesznek részt az adatvédelemmel kapcsolatos feladatok ellátásában:
- (2) **Ügyvezető**
 - a) a Felügyelőbizottság egyetértését követően kijelöli az adatvédelmi tisztviselőt,
 - b) biztosítja az adatvédelmi feladatok ellátásához szükséges tárgyi feltételeket és forrásokat,
 - c) elfogadja az Adatvédelmi és Adatbiztonsági Szabályzatot,
 - d) dönt az adatkezelés bevezetéséről, illetve megszüntetéséről,

- e) gondoskodik az adatvédelmi rendszer időszakos felülvizsgálatáról,
- f) betartatja az adatvédelmi és titokvédelmi szabályokat,
- g) gondoskodik az adatvédelmi nyilvántartások megfelelő vezetéséről,
- h) gondoskodik az adatkezelésben résztvevő személyek (munkavállalók vagy megbízottak) megfelelő tájékoztatásáról és oktatásáról,
- i) gondoskodik az érintett jogainak gyakorlásához szükséges feltételek biztosításáról.

(3) **Rendezvény és Programigazgató**

- a) közreműködik az érintettek adatvédelmi tájékoztatásában (pl. on-line média felületek)
- b) adatvédelmi incidens esetén közreműködik az érintettek tájékoztatásában

(4) **Koordinációs Igazgató**

- a) gondoskodik az információbiztonsággal kapcsolatos feladatokat ellátásáról,
- b) gondoskodik az informatikával kapcsolatos nyilvántartásokat (pl.: jelszavak és jogosultságok nyilvántartása) vezetéséről,
- c) gondoskodik az adatok kezelése során a technikai védelmről,
- d) informatikai jellegű adatvédelmi incidens esetén részt vesz az adatvédelmi incidens kivizsgálásában,
- e) gondoskodik az információbiztonsági előírások megismertetéséről a munkatársakkal.

(5) **Jogtanácsos**

- a) szakmai támogatást nyújt az adatvédelmi tisztviselő részére a nem adatvédelmi tárgyú jogszabályokkal kapcsolatban,
- b) az adatvédelmi tisztviselővel egyeztetve az adatkezelést megalapozó jogi dokumentációt elkészíti (pl. szolgáltatási szerződés, munkaszerződés).

(6) **Titkársági referens**

- a.) megválaszolja az adatkezeléssel és érintetti joggyakorlással kapcsolatos kérelmeket – szükség esetén az adatvédelmi tisztviselő bevonásával
- b.) ellátja az adatkezeléssel kapcsolatos adminisztratív teendőket
- c.) adatkezeléssel összefüggő döntések dokumentálása,
 - érdekmérlegelési teszt elvégzése,
 - hatásvizsgálat lefolytatása,
 - az adatkezeléssel összefüggő szerződések előkészítése,
 - az adatkezelések nyilvántartásának naprakészen tartásához szükséges információk átadása az adatvédelmi tisztviselő részére
 - az érintett hozzájárulásával végzett adatkezelés esetén ellenőrzi, hogy a hozzájárulást szabályosan szerezték-e be
- d.) közreműködik az érintettek tájékoztatásának biztosításában (tájékoztatók kihelyezése, stb.)
- e.) segíti az adatvédelmi tisztviselőt feladatai ellátásában (operatív ügyintézés)

(7) Az Adatvédelmi tisztviselő

Az Adatvédelmi tisztviselő feladatai:

- a) közreműködik az adatvédelemmel kapcsolatos döntések előkészítésében és az érintetti joggyakorlás biztosításában,
- b) tájékoztat és szakmai tanácsot ad az adatkezelést végző munkavállalók és megbízottak részére az adatvédelmi alapelvek és szabályok betartása érdekében
- c) ellenőrzi az adatvédelmi jogszabályoknak, valamint jelen Szabályzatnak a betartását Társaság adatkezelési tevékenysége során
- d) tanácsot ad Ügyvezető részére az adatvédelemmel kapcsolatos feladatkörök kijelölése tárgyában
- e) elősegíti az adatkezelési tevékenységekben résztvevő személyek adatkezelési tudatosság-növelését
- f) időszakos belső adatvédelmi auditot tart az adatkezeléssel kapcsolatos szabálytalanságok feltárása érdekében
- g) időszakos adatvédelmi oktatást tart Társaság munkatársai – illetve szükség esetén megbízottai – részére
- h) kérésre szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, valamint nyomon követi a hatásvizsgálat elvégzését,
- i) együttműködik a felügyeleti hatósággal,
- j) adatkezeléssel összefüggő ügyekben kapcsolattartó pont a felügyeleti hatóság felé
- k) szükség szerint konzultációt folytat a felügyeleti hatósággal,
- l) adatvédelemmel kapcsolatos panasz esetén kivizsgálja a panaszt és jelentést tesz az Ügyvezető felé
- m) előkészíti és aktualizálja az Adatvédelmi és Adatbiztonsági Szabályzatot, melyet Ügyvezető fogad el,
- n) az adatvédelmi incidenssel kapcsolatosan ellátja a jelen Szabályzat szerinti feladatokat
- o) vezeti az Adatkezelési Nyilvántartást,
- p) összefoglaló jelentést készít Ügyvezető részére,
- q) előkészíti az adatvédelmi auditokat,
- r) előkészíti az adatkezeléssel kapcsolatos döntéseket, melynek körében szükség esetén hatásvizsgálatot végez,,
- s) rendszeres időközönként áttekinti a hatásvizsgálatban azonosított kockázatok alakulását, közreműködik az adatvédelmi hatásvizsgálatok utóellenőrzésben,
- t) közreműködik az érintetti joggyakorlás biztosításában,
- u) közreműködik az adatvédelmi incidensek kivizsgálásában,
- v) közreműködik az adatvédelmi auditok lefolytatásában.

(8) Munkavállalók, megbízottak – továbbiakban együttesen munkavállalók – adatkezeléssel kapcsolatos kötelezettségei

A munkavállalók kötelezettsége a jelen Szabályzat adatvédelmi előírásainak ismerete, valamint maradéktalan betartása. A munkavállalók tájékoztatják e körben az Adatvédelmi tisztviselőt a feladatkörükben felmerült bármely adatvédelmi problémáról, esetleges kérdéseiről. A munkatársak kötelezettsége, hogy észrevétel esetén az adatkezeléssel kapcsolatos feltárt visszasságot haladéktanul

megszüntessék, továbbá, hogy részt vegyenek az adatvédelmi oktatáson.

- (a) Az Adatkezelő úgy alakítja ki adatkezelési folyamatait, hogy minden munkavállaló kizárólag azon adatokhoz férjen hozzá, mellyel feladata van.
- (b) Munkavállaló köteles a Társaságnál érvényben lévő adatbiztonsági szabályok megismerésére, betartására és betartatására. Ennek érdekében Társaság jelen Szabályzatot és további szervezet irányító eszközöket minden munkavállaló számára elérhetővé teszi.
- (c) A munkavállaló munkavégzése során köteles a jelen Szabályzat rendelkezései szerint eljárni, valamint figyelembe venni az Adatvédelmi tisztviselő javaslatait és ajánlásait.
- (d) A munkavállalót általános titoktartási kötelezettség terheli a munkavégzése és feladatai végzése során tudomására jutott adatok tekintetében a Munka Törvénykönyve. szerint. A titoktartási kötelezettség a jogviszony megszűnését követően is fennáll.
- (e) Munkavállaló a Társaságnál tudomására jutott személyes adatokat kizárólag munkakörével kapcsolatban, a Társaság céljaival összhangban kezelheti és továbbíthatja. Munkavállaló ezen adatokat jogosultsággal nem rendelkező személynek nem adhatja tovább, a meghatározott céltól eltérően nem kezelheti, másra nem használhatja fel, nem hozhatja nyilvánosságra.
- (f) Amennyiben munkavállaló az adatvédelemre vonatkozó szabályok megsértését észleli, úgy haladéktalanul köteles ezt jelezni adatvédelmi referens vagy Ügyvezető részére.
- (g) Amennyiben munkavállaló a jelen Szabályzat rendelkezéseit szándékosan vagy súlyos gondatlansággal jelentős mértékben megszegi, azzal a munkaviszonyból származó lényeges kötelezettségét szegi meg, így cselekménye az Mt. 179. § alapján munkajogi következményeket vonhat maga után.
- (h) Amennyiben a titoktartási kötelezettség megszegése kimeríti a Btk. 223. §-a szerinti magántitok megsértése bűncselekmény törvényi tényállását - aki a foglalkozásánál fogva tudomására jutott magántitkot alapos ok nélkül felfedi, vétség miatt elzárással büntetendő – Ügyvezető az eset összes körülményét figyelembe véve dönt a büntetőeljárás megindításáról.
- (i) A Társaság kizárólag az Adatkezelési Nyilvántartásban foglaltak szerint kezel adatokat. Az Adatkezelési Nyilvántartásban foglalt adatokon felül bármely adatkezelés esetén munkavállalót terheli a felelősség a jogszerűtlen adatkezelés következményei tekintetében. A jogszerűtlen adatkezeléssel az Társaságnak okozott kár az Mt. 179. § alapján kártérítési felelősséget von maga után.

XI. AZ ADATKEZELÉSI TEVÉKENYSÉGEK BEVEZETÉSE ÉS MEGSZÜNTETÉSE

- (1) Új adatkezelési tevékenység bevezetéséről az Ügyvezető dönt.
- (2) Az adatkezeléssel kapcsolatos döntés előkészítését az adatvédelmi referens végzi, az Adatvédelmi tisztviselő, az adatkezeléssel érintett szervezeti egység vezetőjének, valamint elektronikusan kezelt adat érintettsége esetén az IT szolgáltatást nyújtó szervezet bevonásával. Az Adatvédelmi tisztviselő véleményének kikéréséhez olyan leírást kell benyújtani, amely részletesen meghatározza az adatkezelés célját, jogalapját, a kezelendő adatok körét, és az adatkezelés egyéb feltételeit.

(3) A Társaság hatásvizsgálatot végez, amennyiben az adatkezelés valamely – különösen új technológiákat alkalmazó – típusa –, figyelemmel annak jellegére, hatókörére, körülményére és céljaira, valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve. A hatásvizsgálat célja annak felderítése, hogy az új adatkezelési tevékenység hogyan érinti a személyes adatok védelmét. Kötelező az adatvédelmi hatásvizsgálatot a Rendelet 35. cikk (3) bekezdésében, illetve a Nemzeti Adatvédelmi és Információszabadság Hatóság által közzétett jegyzékben szereplő adatkezelések, adatkezelési műveletek esetén. A hatásvizsgálatot legalább háromévente felül kell vizsgálni, szükség esetén újra el kell végezni,

(4) Amennyiben a Társaság valamely adatkezelésének a Társaság vagy harmadik személy jogos érdeke a jogalapja [Rendelet 6. cikk (1) bekezdés f) pont], abban az esetben érdekmérlegelési tesztet kell elvégezni és ezt dokumentálni. Jogos érdek az a törvényes, kellően pontosan megfogalmazott, valós és fennálló, illetve elérhető előny, amelyet a Társaság – vagy a harmadik személy - származtat származtathat az adatkezelésből. Az érdekmérlegelési tesztet a Társaság – az Adatvédelmi tisztviselő szakmai javaslatai szerint – végzi. Az érdekmérlegelési tesztet írásban kell elvégezni.

(5) Az érdekmérlegelési teszt tartalmát a tervezett adatkezelés függvényében kell meghatározni, azonban minden esetben tartalmaznia kell a következőket:

- a) tervezett adatkezelés leírása, személyes adatok köre
- b) adatkezelő vagy harmadik fél jogos érdekének pontos meghatározása
- c) érintett érdekeinek és jogainak azonosítása
- d) adatkezelő vagy harmadik fél és az érintett érdekeinek összevetése
- e) adatkezeléshez kapcsolódó garanciák
- f) az érdekmérlegelés eredménye

(6) Az új adatkezelésről szóló döntés tartalmazza

- a) érintettek körét
- b) kezelt adatok körét, különös tekintettel arra, hogy személyes adatok különleges kategóriái érintettek-e
- c) adatkezelés célját
- d) adatkezelés jogalapját
- e) az adatok felvételének és törlésének rendjét
- f) az adatok tárolási időtartamát
- g) az adatok tárolásának módját
- h) az adatok címzettjeit
- i) adattovábbítás esetén az erre vonatkozó döntést
- j) alkalmazandóak-e különös biztonsági intézkedések az adatokkal kapcsolatban

(2) Új adatkezelés bevezetése esetén Adatvédelmi tisztviselő – érintett terület vezetőjével együttműködve – előkészíti az adatvédelmi tájékoztatót, és – hozzájáruláson alapuló adatkezelés esetén – a hozzájáruló nyilatkozat mintáját.

(3) A Titkársági referens gondoskodik az adatvédelmi tájékoztató érintettek számára történő elérhetővé tételéről – szükség esetén IT szolgáltatást biztosító szervezet bevonásával a honlapon történő közzétételéről.

- (4) Szerződés teljesítéséhez szükséges adatkezelés esetén jogi munkatárs – adatvédelmi tisztviselő szakmai javaslatai alapján – megszővegezi a szükséges szerződéses rendelkezéseket.
- (5) A végleges dokumentumok szakmai megfelelőségéért a Koordinációs Igazgató, az adatvédelmi megfelelőségéért az adatvédelmi tisztviselő, az informatikai, információbiztonsági megfelelőségért pedig az IT szolgáltatást biztosító szervezet a felelős.
- (6) Új adatkezelési tevékenység esetén IT szolgáltatást biztosító szervezet – Ügyvezető utasítása alapján – gondoskodik a szükséges információbiztonsági intézkedések végrehajtásáról.
- (7) Adatvédelmi tisztviselő az új adatkezelési tevékenységet bevezeti az Adatkezelési Nyilvántartásba. Az adatkezelés megszüntetése esetén az Adatkezelési Nyilvántartásból az egyes adatfajtákat törölni kell.
- (8) Amennyiben a kezelt adatokra a továbbiakban nincs szükség (az adatkezelési cél megvalósult), jogszabályi változások miatt indokolt, illetve az adatvédelmi felügyeleti hatóság vagy bíróság döntése okán az adatok kezelését meg kell szüntetni. Az adatkezelés megszüntetéséről Ügyvezető jogosult dönteni.

XII. TECHNIKAI ÉS SZERVEZÉSI INTÉZKEDÉSEK AZ ADATKEZELÉS SORÁN

- (1) Az adatokat kezelő munkatársak kötelesek a megőrzésre, illetve irattározásra nem kerülő és feleslegessé vált iratok és egyéb nyomtatványok, feljegyzések megsemmisítésére, amelyet – ahol rendelkezésre áll – iratmegsemmisítővel kell végrehajtani. A papírvagdalka a kommunális szemétkébe üríthető. A kommunális szemétkébe ép vagy rekonstruálható formában nem kerülhet személyes vagy egyéb okból nem nyilvános adatot hordozó papír.
- (2) Személyes vagy egyéb okból nem nyilvános adatot tartalmazó dokumentum nem maradhat őrizetlenül folyosón, vagy a nyilvánosság részére nyitva álló helyen. Az irodákat munkaidőn kívül, illetve munkaidőben a munkatársak távollétében kulcsra zárva kell tartani.
- (3) A személyes adatokat tartalmazó iratok nem tárolhatóak nyilvánosság számára nyitva álló helyen, illetve ablakok mellett olyan módon, hogy az illetéktelen személyek számára megismerhetővé váljon.
- (4) Telefonon történő hivatalos beszélgetést csukott ajtók mögött, más személyek kizárásával kell folytatni. Harmadik személy jelenlétében csak a saját ügyében folytatható hivatalos telefonbeszélgetés, ezen kívül általános információk továbbíthatóak harmadik személy részére.
- (5) Mivel a telefon nem alkalmas a telefonáló személy beazonosítására, ezért telefonon csak általános információ adható át, amelyet harmadik személy egyéb nyilvános forrásból is megismerhet. Azonosítatlan személy csak általános tájékoztatásban részesülhet, vagy közérdekű adatigénylés keretében adhatók át részére adatok.
- (6) Személyes adatok továbbítása során az adatkezeléssel megbízott ügyintéző felelős azért, hogy az adatok felfedés nélkül (ép, lezárt borítékban vagy csomagban, kívülről nem olvasható módon) kerüljenek továbbításra címzett részére.
- (7) A Társaság által üzemeltetett Brüsszeli Magyar Ház területén őrizetlenül hagyott, illetve

elveszett, majd megtalált iratokat a Társaság őrzi a személyazonosságát igazoló érintett részére történő átadásig. Az Érintettet az irat előkerüléséről a Társaság munkatársa értesíti. Hatósági személyazonosító okiratok megtalálása esetén azokat a rendőrhatalóság felé kell továbbítani.

(8) Az adatkezelési műveleteket úgy kell megtervezni és végrehajtani, hogy az a vonatkozó jogszabályok alkalmazása során biztosítsa az érintettek magánszférájának védelmét.

(9) Az adatot kezelő személy a tudomására jutott adatot és információt csak a feladatainak ellátására használhatja fel, nem hozhatja illetéktelen személy tudomására, nem adhat ki vezetője engedélye nélkül semmilyen információt.

(10) Az adatot kezelő személy köteles a munkája során tudomására jutott személyes adatot, üzleti titkot, valamint a Társaság tevékenységére vonatkozó alapvető fontosságú információt megőrizni. A munkavállaló ezen túlmenően sem közölhet illetéktelen személlyel olyan adatot, mely munkakörével összefüggésben jutott tudomására, illetve ilyen adatokat személyes célokra nem használhat fel. A titoktartás nem terjed ki a közérdekű adatokra és a közérdekből nyilvános adatokra vonatkozó tájékoztatási kötelezettségre.

XIII. ADATTOVÁBBÍTÁS, ADATFELDOLGOZÓK, KÖZÖS ADATKEZELÉS

(1) A Személyes adatok továbbítására kizárólag a jogszabályok és jelen Szabályzat rendelkezései szerint van lehetőség. Az adattovábbítás feltételeinek, jogalapjának meglétét Adatkezelő minden egyes személyes adattal összefüggésben köteles vizsgálni. Amennyiben az adattovábbításnak nincsenek meg a feltételei, az adat nem továbbítható.

(2) Adatfeldolgozó igénybevétele esetén az Adatkezelő által az adatfeldolgozóval kötendő szerződésnek tartalmaznia kell a Rendelet 28. cikk (1)-(4) bekezdésében foglalt tartalmi elemeket:

- a.) Az adatfeldolgozó megfelelő garanciákat nyújt az adatkezelés Rendelet követelményeinek való megfelelését és az érintettek jogainak védelmét biztosító, megfelelő technikai és szervezési intézkedések végrehajtására
- b.) Az adatfeldolgozó az adatkezelő előzetesen írásban tett eseti vagy általános felhatalmazása nélkül további adatfeldolgozót nem vehet igénybe. Az általános írásbeli felhatalmazás esetén az adatfeldolgozó tájékoztatja az adatkezelőt minden olyan tervezett változásról, amely további adatfeldolgozók igénybevételeit vagy azok cseréjét érinti, ezzel biztosítva lehetőséget az adatkezelőnek arra, hogy ezekkel a változtatásokkal szemben kifogást emeljen.
- c.) Az adatfeldolgozó által végzett adatkezelést olyan - az adatkezelés tárgyát, időtartamát, jellegét és célját, a személyes adatok típusát, az érintettek kategóriáit, valamint az adatkezelő kötelezettségeit és jogait meghatározó - szerződésnek vagy más jogi aktusnak kell szabályoznia, amely köti az adatfeldolgozót az adatkezelővel szemben.

(3) Az adatfeldolgozóval kötendő szerződés különösen előírja, hogy az adatfeldolgozó:

- a) a személyes adatokat kizárólag az adatkezelő írásbeli utasításai alapján kezeli - beleértve a személyes adatoknak valamely harmadik ország vagy nemzetközi szervezet számára való továbbítását is -, kivéve akkor, ha az adatkezelést az adatfeldolgozóra vonatkozó jogszabály

írja elő; ebben az esetben erről a jogi előírásról az adatfeldolgozó az adatkezelőt az adatkezelést megelőzően értesíti, kivéve, ha az adatkezelő értesítését az adott jogszabály fontos közérdekből tiltja;

- b) biztosítja azt, hogy a személyes adatok kezelésére feljogosított személyek titoktartási kötelezettséget vállalnak vagy jogszabályon alapuló megfelelő titoktartási kötelezettség alatt állnak;
- c) meghozza az adatkezelés biztonsága érdekében szükséges, Rendelet 32. cikkben előírt intézkedéseket;
- d) tiszteletben tartja a további adatfeldolgozó igénybevételére vonatkozó feltételeket;
- e) az adatkezelés jellegének figyelembevételével megfelelő technikai és szervezési intézkedésekkel a lehetséges mértékben segíti az adatkezelőt abban, hogy teljesíteni tudja kötelezettségét az érintett jogainak gyakorlásához kapcsolódó kérelmek megválaszolása tekintetében;
- f.) segíti az adatkezelőt az adatbiztonsággal kapcsolatos, Rendelet 32-36. cikk szerinti kötelezettségek teljesítésében, figyelembe véve az adatkezelés jellegét és az adatfeldolgozó rendelkezésére álló információkat;
- g.) az adatkezelési szolgáltatás nyújtásának befejezését követően az Adatkezelő döntése alapján minden személyes adatot töröl vagy visszajuttat az adatkezelőnek, és törli a meglévő másolatokat, kivéve, ha jogszabály a személyes adatok tárolását írja elő;
- h.) az adatkezelő rendelkezésére bocsát minden olyan információt, amely a jelen Szabályzatban foglalt kötelezettségek teljesítésének igazolásához szükséges, továbbá amely lehetővé teszi és elősegíti az adatkezelő által vagy az általa megbízott más ellenőr által végzett auditokat, beleértve a helyszíni vizsgálatokat is.

(4) Ha az adatfeldolgozó az adatkezelő nevében végzett konkrét adatkezelési tevékenységekhez további adatfeldolgozó szolgáltatásait is igénybe veszi, szerződés útján erre a további adatfeldolgozóra is ugyanazok az adatvédelmi kötelezettségeket kell telepíteni, mint amelyek az adatkezelő és az adatfeldolgozó között létrejött szerződésben szerepelnek, különösen úgy, hogy a további adatfeldolgozónak megfelelő garanciákat kell nyújtania a megfelelő technikai és szervezési intézkedések végrehajtására, és ezáltal biztosítania kell, hogy az adatkezelés megfeleljen e rendelet követelményeinek. Ha a további adatfeldolgozó nem teljesíti adatvédelmi kötelezettségeit, az őt megbízó adatfeldolgozó teljes felelősséggel tartozik az adatkezelő felé a további adatfeldolgozó kötelezettségeinek a teljesítéséért.

(5) Az adatfeldolgozási szerződésben rögzíteni kell továbbá

- a) az adatfeldolgozó kötelezettségét a hozzá érkező adatvédelmi tárgyú kérelmek adatkezelő részére történő továbbítására vonatkozóan;
- b) adatfeldolgozó közreműködési kötelezettségét adatvédelmi incidens esetén
- c) adatfeldolgozó együttműködési kötelezettségét hatásvizsgálat végzése során
- d) adatkezelő és az adatvédelmi tisztviselő elérhetősége, az adatvédelmi felügyeleti hatóság elérhetősége).

(6) A Titkársági referens az adatfeldolgozó adatait átadja Adatvédelmi tisztviselő részére, aki felvezeti az Adatkezelési Nyilvántartásba.

(7) Az Adatkezelő főszabály szerint nem továbbít adatot harmadik országba. Amennyiben eseti jelleggel ilyen adattovábbításra sor kerül, az Adatkezelő kiemelt figyelmet fordít érintettek tájékoztatására és – szükség esetén – hozzájárulásuk dokumentálására.

(8) Ha az adatkezelés céljait és eszközeit két vagy több adatkezelő közösen határozzák meg, közös adatkezelőnek minősülnek. A közös adatkezelők átlátható módon, a közöttük létrejött megállapodásban határozzák meg a Rendelet szerinti kötelezettségeik teljesítéséért fennálló, különösen az érintett jogainak gyakorlásával és a Rendelet 13. és 14. cikkében említett információk rendelkezésre bocsátásával kapcsolatos feladataikkal összefüggő felelősségük megosztását. A megállapodásnak megfelelően tükröznie kell a közös adatkezelők érintettekkel szembeni szerepét, és a velük való kapcsolatukat. A megállapodás lényegéről az érintettet tájékoztatni kell.

XIV. AZ ADATVÉDLEMI OKTATÁS

(1) Az adatvédelmi oktatás célja, hogy biztosítsa, hogy munkavállalók és egyéb jogviszonyban foglalkoztatott, személyes adatok kezelését végző személyek az adatkezelés során a jogszabályokat és jelen Szabályzatot maradéktalanul betartsák.

(2) Adatvédelmi tisztviselő – a munkatársak adatvédelmi tudatosságának felmérését követően – dönt a szükséges oktatásról.

(3) Az Adatvédelmi tisztviselő évente egy alkalommal oktatást tart az adatvédelmi tudatosság emelése érdekében, melyen kötelesek részt venni a Társaság adatok kezelésében résztvevő munkatársai.

(4) Az adatvédelmi tisztviselő rendkívüli oktatást tarthat az alábbi esetekben:

a) adatvédelmi incidens megtörténte

b) NAIH eljárás Adatkezelővel szemben

c) adatvédelmi bírság kiszabása olyan szervezettel szemben, ami a Társasággal azonos tevékenységi körben működik

(5) Oktatás tartható élőszóban, írásbeli oktatási anyag átadásával vagy on-line előadás formájában. Az Adatvédelmi tisztviselő az oktatásról jegyzőkönyvet készít.

(6) Az oktatás megszervezése az Adatvédelmi tisztviselő és a Koordinációs Igazgató kötelezettsége.

XV. ZÁRÓ RENDELKEZÉSEK

1. A Szabályzat megállapítása és módosítása

A Szabályzat megállapítására és módosítására a Társaság Ügyvezetője jogosult.

2. Intézkedések a Szabályzat megismertetése vonatkozásában

E Szabályzat rendelkezéseit meg kell ismertetni a Társaság valamennyi munkavállalójával, közreműködőjével (foglalkoztatottjával), azzal, hogy a foglalkoztatásra/ munkavégzésre irányuló szerződésekben elő kell írni, hogy betartása és érvényesítése minden munkavállaló, közreműködő (egyéb foglalkoztatott) lényeges munkaköri kötelezettsége.