A PortfoLion Kockázati Tőkealap-kezelő Zrt.

Adatvédelmi utasítása

Vezérigazgatói utasítás 1/2018 (05.23.)

A jelen utasítást a PortfoLion Zrt. vezérigazgatója adta ki 2018. május 23-án és ennek jeléül aláírta:

Hatálybalépés: 2018. május 23.

…….

Molnár András

Vezérigazgató

Tartalom

I. BEVEZETŐ RENDELKEZÉSEK

(1) A jelen vezérigazgatói utasítás (továbbiakban: utasítás) célja, hogy összefoglalja a PortfoLion Kockázati Tőkealap-kezelő Zrt. (a továbbiakban: Társaság) által a Társaság működése, tevékenységének ellátása, szolgáltatásának nyújtása során gyűjtött, rendelkezésre bocsátott vagy egyéb módon tudomására jutott személyes adatok kezelésével kapcsolatos egyes lényeges rendelkezéseket, különösen az adatvédelmi tevékenység ellátásában résztvevő munkatársak feladatait és együttműködésük kereteit.

II. ALAPELVEK

(2) A Társaság a személyes adatok kezelésével járó tevékenysége során érvényre juttatja a GDPR-ban foglalt alapelveket, így különösen:

a/ jogszerűség, tisztességes eljárás és átláthatóság elve: a személyes adatok kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni;

b/ célhoz kötöttség elve: a személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történik, és azokat a Társaság nem kezeli ezekkel a célokkal össze nem egyeztethető módon;

c/ adattakarékosság elve: a kezelt személyes adatok az adatkezelés céljai szempontjából megfelelőek és relevánsak kell, hogy legyenek, és a szükségesre kell korlátozódniuk;

d/ pontosság elve: a kezelt személyes adatoknak pontosnak és szükség esetén naprakésznek kell lenniük; minden ésszerű intézkedést meg kell tenni annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul töröljék vagy helyesbítsék;

e/ korlátozott tárolhatóság elve: a személyes adatok tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé;

f/ integritás és bizalmas jelleg: a személyes adatok 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;

g/ beépített adatvédelem elve: olyan megfelelő technikai és szervezési intézkedések végrehajtása, amelyek már az adatkezeléssel járó folyamatok tervezésétől (az adatkezelés módjának meghatározásától) kezdődően az adatkezelés megszüntetéséig terjedő időszakban azt célozzák, hogy az adatvédelmi elvek hatékony megvalósítása, illetve a GDPR-ban foglalt követelmények teljesítéséhez

és az érintettek jogainak védelméhez szükséges garanciák beépüljenek az adatkezelés folyamatába;

h/ alapértelmezett adatvédelem elve: olyan technikai és szervezési intézkedéseket végrehajtása, amelyek biztosítják, hogy alapértelmezés szerint kizárólag olyan személyes adatok kezelésére kerüljön sor, amelyek az adott konkrét adatkezelési cél szempontjából szükségesek, továbbá, hogy a gyűjtött személyes adatok mennyisége, kezelésük mértéke, tárolásuk időtartama és hozzáférhetőségük is csak az adatkezelési cél cél szempontjából szükséges mértékre korlátozódjon. Különösen azt kell biztosítani, hogy a személyes adatok alapértelmezés szerint természetes személy beavatkozása nélkül ne válhassanak hozzáférhetővé meghatározatlan számú személy számára.

III. ADATVÉDELMI DOKUMENTÁCIÓ

(3) A Társaság az adatkezelést érintő minden tevékenységről, beleértve az adatkezelés megkezdésére, megváltoztatására irányuló bármely és valamennyi igényt, szándékot, az adatkezelést érintő valamennyi és bármely döntést írásban, dokumentálható és visszakereshető formában rögzíti és tárolja.

(4) A Társaságnak képesnek kell lennie annak igazolására, hogy az érintett személyes adatainak kezeléséhez hozzájárult. Amennyiben az adatkezelés jogalapja az érintett hozzájárulása, úgy a hozzájárulás visszavonása esetén a Társaság a hozzájárulás alapján kezelt adatokat a GDPR 17. cikke figyelembe vételével törli.

(5) A Társaság megfelelő intézkedéseket hoz annak érdekében, hogy az érintett részére a személyes adatok kezelésére vonatkozó valamennyi szükséges információt és minden egyes tájékoztatást tömör, átlátható, érthető és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazva nyújtsa, különösen a gyermekeknek címzett bármely információ esetében. Az érintettnek címzett tájékoztatás megtörténtét és annak az érintett általi megismerését dokumentálható és visszakereshető formában rögzíteni kell.

(6) A Társaság a GDPR 30. cikk szerinti adatkezelési nyilvántartást nem köteles vezetni, de az adatkezelési tevékenységeiről elektronikus formában nyilvántartást egyszerűsített nyilvántartást vezet.

IV. ADATVÉDELMI KOORDINÁTOR

(7) A Társaság adatvédelmi koordinátori feladatait az irodavezető látja el.

(8) Az adatvédelmi koordinátor:

a/ a jelen utasításban meghatározott feladatok ellátásával elősegíti a Társaság adatvédelmi megfelelőségének biztosítását, így különösen:

aa/ ellenőrzi a GDPR-nak, valamint az egyéb uniós vagy nemzeti adatvédelmi rendelkezéseknek, továbbá a Társaság személyes adatok védelmével kapcsolatos belső szabályainak való megfelelést,

ab/ tájékoztatást és szakmai tanácsot ad a munkatársaknak a személyes adatok kezelésével kapcsolatos szabályok alkalmazásáról,

ac/ elősegíti a Társaság alkalmazottai adatvédelmi tudatosságának növelését,

ad/ irányítja az érintettől származó kérelmek, panaszok megválaszolását,

ae/ kapcsolatot tart az adatvédelmi felügyeleti hatósággal és adatvédelmi külső szakértővel;

b/ koordinálja az adatvédelmi tevékenység irányításában és ellátásában részt vevő szervek adatvédelemmel összefüggő tevékenységét;

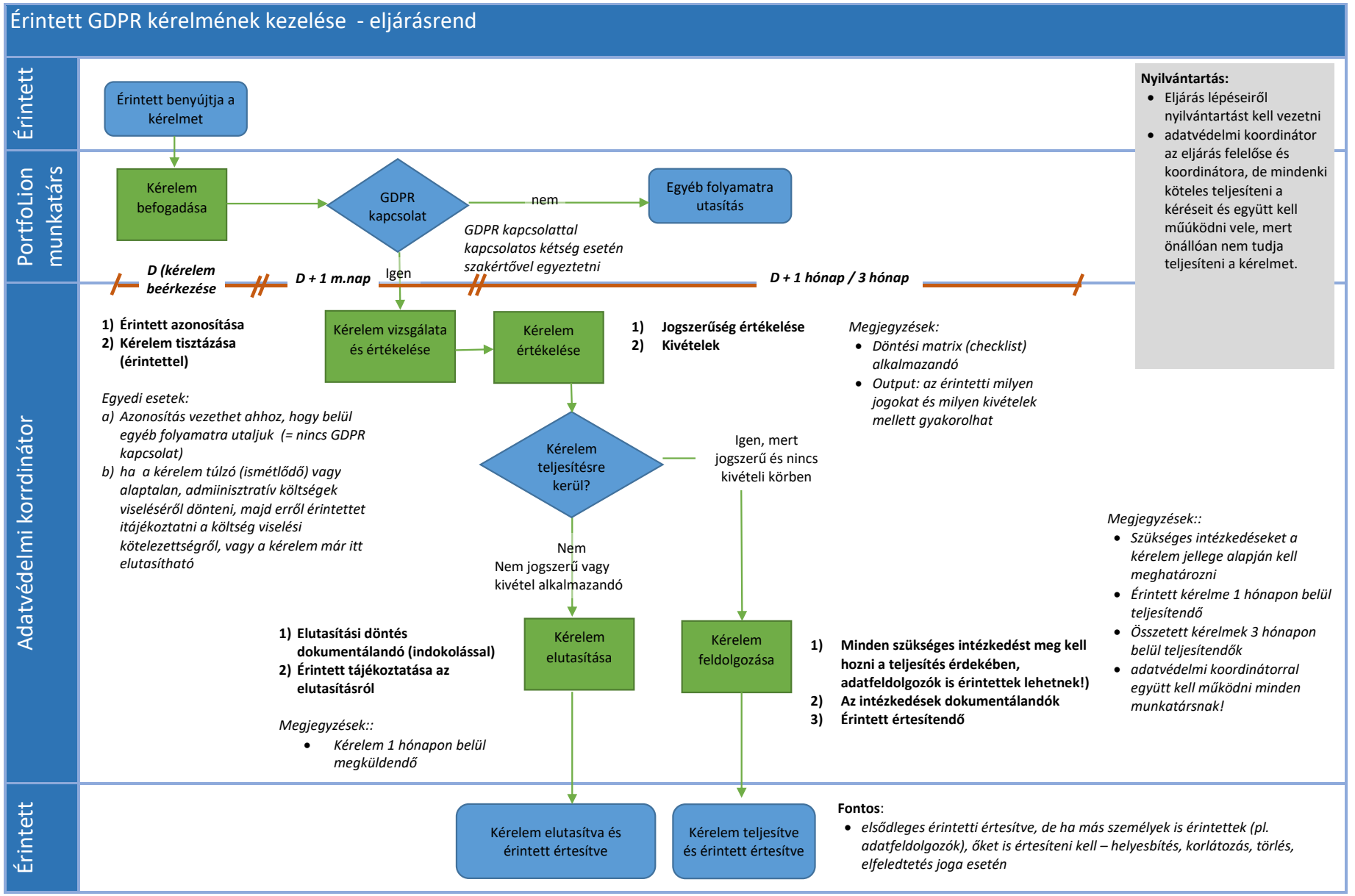
c/ szükség esetén projekt indítását kezdeményezi az adatvédelmi követelményeknek való megfelelés biztosítása érdekében.

V. AZ ÉRINTETTŐL SZÁRMAZÓ KÉRELMEK, PANASZOK MEGVÁLASZOLÁSÁNAK RENDJE

(1) Az érintett jogai röviden a következők: tájékoztatáshoz való jog, hozzáférési joghelyesbítéshez való jog, törléshez való jog, elfeledtetéshez való jog, korlátozáshoz való jog, a személyes adatok helyesbítéséről, törléséről, az adatkezelés korlátozásáról tájékoztatott címzettekről történő tájékoztatáshoz való jog, adathordozhatósághoz való jog, tiltakozáshoz való jog, az érintett joga arra, hogy ne terjedjen ki rá a kizárólag automatizált adatkezelésen alapuló döntés hatálya, jogorvoslathoz való jog.

(2) A Társaság biztosítja az érintetteket megillető adatvédelmi jogok érvényesülését az alábbi folyamat bevezetésével.

Érintett GDPR kérelmének kezelése - eljárásrend



VI. ADATFELDOLGOZÓI SZERZŐDÉSEK MEGKÖTÉSÉNEK SZABÁLYAI

(3) Adatfeldolgozó [(22) bekezdés] igénybe vétele esetén az adatfeldolgozóval kötendő szerződésnek tartalmaznia kell a GDPR 28. cikk (1)-(4) bekezdésében foglalt tartalmi elemeket a (4) bekezdésben foglalt kiegészítések és pontosítások szerint.

(4) Az adatfeldolgozóval kötendő szerződésben

a/ a kellő részletességgel (pl. szabályzatra vagy szabványokra utalással) meg kell határozni az adatfeldolgozó, vagy az adatfeldolgozó által igénybe veendő további adatfeldolgozó (al-adatfeldolgozó) által betartandó adatbiztonsági szabályokat, amelyek nem lehetnek kevésbé szigorúak, mint a Társaság által alkalmazott adatbiztonsági intézkedések, és az adatfeldolgozónak az adatbiztonsági intézkedések végrehajtásával kapcsolatos feladatait;

b/ rögzíteni kell az adatfeldolgozónak az érintettől származó kérelmek, panaszok megválaszolásában való közreműködésének eljárásrendjét;

c/ rögzíteni kell az adatfeldolgozó kötelezettségeit adatvédelmi rendellenesség vagy incidens észlelése esetén, így különösen

ca/ az adatvédelmi rendellenesség vagy incidens tudomásra jutása esetén a Társaság adatvédelmi koordinátorát haladéktalanul köteles értesíteni az adatvédelmi incidensről,

cb/ köteles együttműködni a Társaság adatvédelmi koordinátorával és más közreműködő szervezeti egységgel az adatvédelmi rendellenesség vagy incidens okának feltárásban és következményeinek felszámolásában,

cc/ az adatvédelmi incidens bejelentésének teljesítésében,

d/ rögzíteni kell az adatfeldolgozó kötelezettségét az adatvédelmi hatásvizsgálat elvégzésében, illetve a hatásvizsgálatban azonosított kockázatok alakulásának figyelemmel kísérésében, az adatkezeléssel járó kockázatok változásának jelzésében, illetve az adatvédelmi hatásvizsgálatok utóellenőrzésben.

VII.AZ ADATVÉDELMI RENDELLENESSÉGEK ÉS INCIDENSEK KEZELÉSE

(5) Adatvédelmi incidens csak akkor következik be, ha az adatbiztonsági intézkedések – akár vétlen, akár szándékos – megsértésének következtében bekövetkezik a személyes adatok véletlen vagy jogellenes megsemmisítése, elvesztése, megváltoztatása, jogosulatlan közlése vagy az azokhoz való jogosulatlan hozzáférés.

(6) Adatvédelmi rendellenességnek minősül különösen:

a/ a személyes adatok kezelésére vonatkozó adatbiztonsági intézkedések minden olyan – akár vétlen, akár szándékos – sérülése, megszegése, amely nem eredményezi a személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést, de ennek lehetősége fennáll;

b/ a személyes adatok kezelésére vonatkozó adatbiztonsági intézkedéseken kívüli adatvédelmi szabályok megsértése, pl. személyes adatok megfelelő jogalap nélküli kezelése (felvétele, tárolása, továbbítása stb.), a szükségesnél több adat kezelése, a személyes adatoknak az adatmegőrzési határidőn túli kezelése. E pont alá tehát jogvitás esetek tartoznak.

(7) Az adatok véletlen vagy jogellenes megsemmisítésének az adatok – szabályszerű selejtezési, törlési eljáráson kívüli – helyreállíthatatlan megváltoztatása vagy az adatokat tartalmazó adathordozó – nem szabályos selejtezési eljárás során történt – fizikai megsemmisítése, használhatatlanná tétele minősül. Az adat véletlen vagy jogellenes törlése akkor is adatvédelmi incidens, ha a törölt adatot, illetve a megsérült adathordozón lévő adatot úgy sikerül maradéktalanul helyreállítani, hogy az az érintett számára semmilyen következménnyel nem jár, azt nem is észleli.

Az adatok elvesztésének az adatoknak, illetve az adatot tartalmazó adathordozónak a Társaság birtokából való időleges vagy végleges kikerülése minősül, akkor is, ha a Társaság birtokába visszakerült adaton később semmilyen módosítás nem állapítható meg. A Társaság tulajdonát képező, személyes adatokat tartalmazó eszközök, adathordozók, illetve személyes adatokat tartalmazó információs rendszerek elérésére alkalmas eszközök eltulajdonítása is e körbe tartozik. Ezt a szabályt a Társaság tulajdonát képező adathordozókra, mobiltelefonra, laptopra, egyéb számítástechnikai eszközre, továbbá a Társaság alkalmazottainak olyan saját tulajdonú eszközeire (adathordozókra, mobiltelefonra, laptopra, egyéb számítástechnikai eszközre), amelyeket munkavégzéshez, munkaköri feladatok ellátásához, hivatalos célból használhat.

Jogosulatlan közlésnek az adatoknak olyan harmadik személy tudomására hozása minősül (akár szóban, akár írásban, elektronikus vagy bármely más úton), aki az adatokat nem ismerhette volna meg E fejezet alkalmazása szempontjából harmadik személy a Társaság alkalmazottain és az érintetten kívül minden más személy. Jogosulatlan hozzáférésnek minősül minden olyan eset, amikor arra nem jogosult személyek – nekik címzett közlés nélkül is – megismerik a személyes adatot (pl. személyes adatot tartalmazó dokumentum felügyelet nélkül hagyása, , vagy nyilvános internetes felületen, stb.)

(8) Személyes adat véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést vagy annak közvetlen veszélyének fennállását a tudomásra jutást követően haladéktalanul köteles bejelenteni az adatvédelmi koordinátornak.

Az adatvédelmi koordinátor a közvetlenül hozzá érkezett bejelentéseket megvizsgálja. Az adatvédelmi esemény bejelentését követően az adatvédelmi koordinátor:

a/ az adatvédelmi esemény jellegétől függően értesíti a Vezérigazgatót és ;

b/ azon munkatársat, aki részéről közreműködés szükséges az adatvédelmi esemény

(9) Az adatvédelmi esemény körülményeinek feltárásában az adatvédelmi koordinátor, a Társaság valamennyi munkatársa köteles közreműködni. Ennek keretében köteles az adatvédelmi koordinátor által kért adatokat, információkat, bizonyítékokat a kért határidőre rendelkezésre bocsátani, különösen

a/ az adatvédelmi eseménnyel érintett természetes személyek köre és száma;

b/ az adatvédelmi eseménnyel érintett személyes adatok fajtája (beleértve az azonosíthatóság mértékének a meghatározását is) és köre, valamint hozzávetőleges száma;

c/ az adatvédelmi esemény észlelésének időpontja és fennállásának időtartama;

d/ az adatvédelmi esemény részletes leírása, körülményei [mely adatbiztonsági előírás sérült, milyen cselekmény(ek) vagy mulasztás(ok) vezetett/vezettek az adatvédelmi rendellenességhez/incidenshez],

e/ az adatvédelmi esemény lehetséges vagy már bekövetkezett következményei (pl. vagyoni vagy nem vagyoni kár, személyazonosság-lopás vagy a személyazonossággal való visszaélés, pénzügyi veszteség) és hatásai;

f/ az adatvédelmi esemény következményeinek elhárítása érdekében tervezett vagy más megtett intézkedések.

(10) Az adatvédelmi koordinátor vizsgálata során, illetve eredményeként

a/ dönt arról, hogy a bejelentésben leírt eset adatvédelmi rendellenességnek vagy adatvédelmi incidensnek minősül-e;

b/ az adatvédelmi incidens e jellegének megállapítása esetén – szükség esetén – tájékoztatja a Vezérigazgatót az adatvédelmi incidensről, annak súlyosságáról, a lehetséges következményekről, a következmények mérséklésére tett, illetve teendő intézkedésekről;

c/ közreműködik a riportok, tájékoztatások előkészítésében;

d/ dönt arról, hogy az adatvédelmi incidens bejelentendő-e a Nemzeti Adatvédelmi és Információszabadság Hatóságnak, és szükség esetén a Vezérigazgató jóváhagyásával az adatvédelmi incidenst bejelenti a Hatóságnak;

e/ dönt az érintettek tájékoztatásának szükségességéről és jogi tartalmáról (GDPR 34. cikk), az érintettek tájékoztatásának módjáról, és előkészíti a tájékoztató formaszövegét;

f/ nyilvántartást vezet az adatvédelmi incidensekről, feltüntetve az adatvédelmi incidenshez kapcsolódó tényeket, annak hatásait és az orvoslására tett intézkedéseket [GDPR 33. cikk (5) bek.];

g/ javaslatot tehet az adatvédelmi esemény kiváltó okai kiküszöbölésére alkalmas adatbiztonsági intézkedésekre, a meglévő intézkedések módosítására;

h/ amennyiben sajtóközlemény kiadása szükséges, közreműködik a sajtóközlemény előkészítésében.

(11) Az adatvédelmi incidenst az adatvédelmi koordinátor – ha lehetséges – a tudomásszerzést követő 72 órán belül bejelenti az adatvédelmi felügyeleti hatóság felé. Amennyiben a bejelentés megtétele 72 órán belül nem lehetséges, az adatvédelmi koordinátor összegyűjti a késedelem alapjául szolgáló indokokat, bizonyítékokat az adatvédelmi incidensek kivizsgálásában résztvevő szervezeti egységektől. A bejelentést az adatvédelmi koordinátor adatvédelmi felügyeleti hatóság online felületén teszi meg:

(12) A bejelentésnek tartalmaznia kell:

a/ az adatvédelmi koordinátor nevét és elérhetőségét,

b/ az adatvédelmi incidens bekövetkezésének időpontját,

c/ az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek körét és nagyságát,

d/ az adatvédelmi incidenssel érintett adatok kategóriáit és hozzávetőleges számát,

e/ az adatvédelmi incidensből eredő, valószínűsíthető következményeket,

f/ az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

(13) Amennyiben a fenti információk egyidejű közlése nem lehetséges, úgy azokat az adatvédelmi koordinátor indokolatlan késedelem nélkül később részletekben közli a hatósággal.

(14) A Társaság az érintettet az adatvédelmi koordinátornak írásban/e-mail útján/telefonon/SMS útján közvetlenül tájékoztatja az adatvédelmi incidensről az érintett által korábban megadott elérhetőségeken.

(15) A tájékoztatásnak tartalmaznia kell az adatvédelmi incidens jellegét és legalább a (12) bekezdés a/, d/ és e/ pontjában foglalt információkat.

(16) Az adatvédelmi incidensről külső harmadik személyek felé bármilyen kommunikációt csak a Vezérigazgató végezhet.

VIII. AZ ADATBIZTONSÁGI INTÉZKEDÉSEK (TECHNIKAI ÉS SZERVEZÉSI INTÉZKEDÉSEK) MEGHATÁROZÁSA ÉS VÉGREHAJTÁSA

(17) Az adatbiztonsági intézkedések leírását az Informatikai Szabályzat tartalmazza.

IX. ZÁRÓ RENDELKEZÉSEK

(18) Ez a vezérigazgatói utasítás 2018. május 23-én lép hatályba.

1. SZ. MELLÉKLET: ÉRTELMEZŐ RENDELKEZÉSEK

(19) adat: az adatfajta értéke egy adott személy esetén; az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas (MSZ ISO 2382-1 alapján);

(20) adatcsoport: azonos ismérvekkel jellemezhető több adat együttesen (pl. személyazonosító adatok, jövedelmi adatok, stb.);

(21) adatfajta: a kezelt személyes adatok típusának legkisebb egysége (pl. név, születési név, lakcím, telefonszám, havi jövedelem, stb.), ami a nyilvántartási rendszer felhasználói felületén egy rekordon belül rendszerint egy mezőt képez;

(22) adatfeldolgozó: az a természetes, vagy jogi személy, közhatalmi szerv, ügynökség, vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel;

(23) adathordozhatóság: hozzájáruláson vagy szerződésen alapuló, automatizált módon történő adatkezelés [GDPR 6. cikk (1) bek. a) és b) pont, 9. cikk (2) bek. a) pont] esetén az érintett azon joga, hogy a rá vonatkozó, általa az adatkezelő rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja, továbbá azokat egy másik adatkezelőnek továbbítsa;

(24) adatkezelés: a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés, továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés;

(25) adatkezelési cél: az a pontosan meghatározott, jogszerű cél, amelynek elérése érdekében a személyes adatokon az adatkezelő az adatkezelési műveleteket végzi;

(26) adatkezelő: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség, vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza. A Társaság szervezeti egységei által elhatározott vagy jogszabály rendelkezése alapján ellátott adatkezelések tekintetében a Társaság minősül adatkezelőnek;

(27) adattovábbítás: az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele. A Társaság egyes szervezeti egységei közötti, illetve az adatfeldolgozónak történő adatátadás nem minősül adattovábbításnak;

(28) adatvédelem: a személyes adatok jogszerű kezelését és feldolgozását, az adatok biztonságát, valamint az érintett személyek magánszférájának és személyhez fűződő jogainak védelmét biztosító alapelvek, szabályok, eljárások, adatkezelési eszközök, technikai és szervezeti intézkedések és módszerek összessége;

(29) adatvédelmi esemény: az adatvédelmi rendellenesség és az adatvédelmi incidens;

(30) adatvédelmi felügyeleti hatóság: a Nemzeti Adatvédelmi- és Információszabadság Hatóság, illetve a GDPR 56. cikke szerinti fő felügyeleti hatóság;

(31) adatvédelmi koordinátor: olyan személy, akit a Társaság munkaköri leírásban kijelöl adatvédelmi kapcsolattartói feladatokkal;

(32) érintett: azonosított vagy azonosítható természetes személy; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható;

(33) 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)

(34) hozzájárulás: az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez;

(35) munkavállaló: a Társasággal munkaviszonyban álló természetes személy;

(36) személyes adat: azonosított vagy azonosítható természetes személyre (érintett) vonatkozó bármely információ;

(37) személyes adatok különleges kategóriái (különleges adat): a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a természetes személyek egyedi azonosítását célzó genetikai és biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok

(38) természetes személyazonosító adatok: az 1996. évi XX. törvény 4. § (4) bekezdése szerinti adatok (az érintett családi és utóneve, születési családi és utóneve, születési helye, születési ideje és anyja születési családi és utóneve);

(39) titkosítás: az adatok olyan transzformációja, melynek során az adat értelmezhetetlenné válik a megfelelő kulcs ismerete nélkül;

(40) törlés: az adat felismerhetetlenné tétele oly módon, hogy a helyreállítása a továbbiakban már nem lehetséges, amely megvalósulhat adat szintjén, adatcsoport szintjén, egy személyhez kapcsolódó valamennyi adat szintjén, adatbázis/nyilvántartási rendszer része vagy egésze szintjén. A törlés célja megvalósítható deperszonalizálással (aninomizálással) is.