BKV PANORÁMA KFT.

TÁRSASÁGI ADATVÉDELMI ÉS ADATBIZTONSÁGI SZABÁLYZAT

2019.
Felülvizsgálva 2025.01.31

Tartalomjegyzék

Tartalomjegyzék 2

I. FEJEZET ÁLTALÁNOS RENDELKEZÉSEK 5

1. A szabályzat célja 5
2. A Szabályzat hatálya 5
   a) Személyi hatály 5
   b) Tárgyi hatály 5
3. A Szabályzat aktualizálása 5
4. Fogalmak 6

II. FEJEZET AZ ADATVÉDELEMRE VONATKOZÓ ÁLTALÁNOS SZABÁLYOK 14

1. Társaságunk, mint adatkezelő feladatai 14
2. Beépített és alapértelmezett adatvédelem 14
3. A Társaságnál kezelt adatok osztályozása 14
   a) Személyes adat 14
   b) Különleges adat 14
   c) Magántitok, levéltitok 15
   d) Üzleti titok 15
4. Az adatokhoz tartozó adatvédelmi, bizalmassági kategóriák 16
   a) Nyilvános 16
   b) Belső 16
   c) Fokozott bizalmasságú 16
   d) Kiemelt bizalmasságú 16
5. Az egyes adatkezelést végző szervezeti egységek vezetőjének feladatai 17

III. FEJEZET A SZEMÉLYES ADATOK KEZELÉSÉRE VONATKOZÓ SZABÁLYOK 18

1. A személyes adatok kezelésére vonatkozó elvek 18
2. A személyes adatok kezelésének feltételei 18
3. A hozzájárulás feltételei 21
4. A büntetőjogi felelősség megállapítására vonatkozó határozatokra és a bűncselekményekre, illetve a kapcsolódó biztonsági intézkedésekre vonatkozó személyes adatok 22
5. Azonosítást nem igénylő adatkezelés 22
6. Átlátható tájékoztatás, kommunikáció, az érintettek jogainak gyakorlására vonatkozó rendelkezések 22
7. Tájékoztatás és a személyes adatokhoz való hozzáférés 24
   7.1. Az érintettek rendelkezésére bocsátandó információk, ha a személyes adatokat az érintettől gyűjtik 24
   7.2. Az érintettek rendelkezésére bocsátandó információk, ha a személyes adatokat nem az érintettől szerezték meg 25
8. Egyes kiemelt személyes adatkezelések társasági szabályai 26
   a) Munkaviszony létesítése, módosítása, megszűnése kapcsán történő adatkezelés 26
   b) Munkabér, egyéb járandóság, illetőleg a munkaviszony kapcsán keletkező egyéb adatok kezelése 27

c) Videómegfigyelő-rendszerek működtetése 27
d) Társasági testületi üléseken, érdekképviseleti egyeztetéseken történő hangrögzítés . 30
9. Érintettek jogai és érvényesítésük 30
a) Tájékoztatásra, illetve betekintésre irányuló kérelem 30
b) Helyesbítéshez való jog 31
c) Törléshez való jog 31
d) Az adatkezelés korlátozásához való jog 32
e) Az adathordozhatósághoz való jog 33
f) Tiltakozáshoz való jog 33
g) Automatizált döntéshozatal egyedi ügyekben, beleértve a profilalkotást 34
h) A személyes adatokkal összefüggő jogok érvényesítése az érintett halálát követően . 34
10. Adatközlések 35
a) Személyes adat nyilvánosságra hozatala 35
b) Az Európai Unión belüli adattovábbítások (beleértve a belföldre irányuló adattovábbításokat) 35
c) Harmadik (Európai Unión kívüli) országba vagy nemzetközi szervezet részére történő adattovábbítások 36
11. Közös adatkezelés 38
12. Az adatfeldolgozó igénybevételének szabályai 39
a) Társaságunk felelőssége 39
b) Az adatfeldolgozó felelőssége 39

IV. FEJEZET A KÖZÉRDEKŰ ADATOK NYILVÁNOSSÁGÁRA VONATKOZÓ ELŐÍRÁSOK 40

V. FEJEZET AZ ADATBIZTONSÁG ÉS TECHNIKAI HÁTTERÉNEK EGYES KÉRDÉSEI, IRATMINŐSÍTÉSI ALAPELVEK 43

1. Az adatkezelés biztonsága 43
2. Az adatvédelmi incidensek kezelése 44
3. Az infrastruktúrához kapcsolódó védelmi intézkedések 46
a) Szervertermek üzemeltetési rendje, biztonsági előírásai 46
b) Adatok, adatcsoportok besorolása információbiztonsági szempontból 46
4. A hardverekhez kapcsolódó védelmi intézkedések 48
5. A szoftverekhez kapcsolódó védelmi intézkedések 48
6. Katasztrófahelyzetek kezelése 48
7. Az adathordozókhoz kapcsolódó védelmi intézkedések 48
8. Az információ kezelésével kapcsolatos intézkedések 48
9. Személyes adatok törlése az adatkezelés jogalapjának megszűnését követően 49
10. Iratminősítési alapelvek 50
11. Az üzleti titok (II.3.d) pont) és a munkakör betöltésével összefüggésben a munkavállalók tudomására jutott adatok védelme 50

VI. FEJEZET AZ ADATVÉDELMI TISZTVISELŐ FELADATAI, JOGAI, KÖTELEZETTSÉGEI ÉS FELELŐSSÉGE 52

1. Az adatvédelmi tisztviselő jogállása 52
2. Az adatvédelmi tisztviselő feladatai 52
3. Az adatvédelmi tisztviselő jogai 53
4. Az adatvédelmi tisztviselő kötelességei 54
5. Az adatvédelmi tisztviselő felelőssége 55

VII. FEJEZET AZ ADATVÉDELMI ELLENŐRZÉSBEN ÉRINTETTEK JOGAI, KÖTELEZETTSÉGEI ÉS FELELŐSSÉGE 56

1. Az adatvédelmi ellenőrzésben érintett szervezet vezetőinek és munkavállalóinak kötelessége 56
2. Az adatvédelmi ellenőrzésben érintett szervezet vezetőinek és munkavállalóinak jogai 56
3. Az adatvédelmi ellenőrzést kezdeményező vezető kötelessége 57

VIII. FEJEZET AZ ADATKEZELÉSI TEVÉKENYSÉGEK NYILVÁNTARTÁSA 58

IX. FEJEZET ADATVÉDELMI HATÁSVIZSGÁLAT ÉS ELŐZETES KONZULTÁCIÓ..... 60

X. FEJEZET RENDELKEZŐ RÉSZ 62

TITOKTARTÁSI NYILATKOZAT..... 64
JEGYZŐKÖNYV MEGKERESÉS ALAPJÁN AZ EURÓPAI UNIÓN BELÜL TELJESÍTETT ADATTOVÁBBÍTÁSRÓL..... 65
JEGYZŐKÖNYV EURÓPAI UNIÓN KÍVÜLI ORSZÁGBA VAGY NEMZETKÖZI SZERVEZET RÉSZÉRE TÖRTÉNŐ ADATTOVÁBBÍTÁSRÓL 67

I. FEJEZET

ÁLTALÁNOS RENDELKEZÉSEK

1. A szabályzat célja

Jelen szabályzat (a továbbiakban: Szabályzat) célja, hogy – megfelelve a 2018. május 25. napjától kötelezően alkalmazandó, az Európai Parlament és a Tanács 2016. április 27-i (EU) 2016/679. számú, 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 rendeletének (a továbbiakban: Rendelet), valamint az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvénynek (a továbbiakban: Infotv.) – meghatározza a BKV Panoráma Kft. (a továbbiakban: Társaság) által végzett adatkezelésnek, adatfeldolgozásnak és az adatok nyilvántartásának, védelmének törvényes rendjét, valamint biztosítsa az adatvédelem alkotmányos elveinek, az információs önrendelkezési jognak, az információszabadságnak és az adatbiztonság követelményeinek érvényesülését.

Fentiek teljesülése érdekében a felmerülő adatvédelmi és adatbiztonsági feladatokra tekintettel, a Társaság által történő adatkezelések szabályszerűségének biztosítása érdekében a következők szerint rendelkezem.

2. A Szabályzat hatálya

a) *Személyi hatály*

A Szabályzat személyi hatálya a Társaság vezető tisztségviselőire és munkavállalóira terjed ki.

b) *Tárgyi hatály*

A Szabályzat tárgyi hatálya kiterjed a Társaság területén felvételezett, feldolgozás alatt lévő, a tárolt és a feldolgozás (azaz adatkezelés és -feldolgozás) során létrejött adatokra, illetve adathordozókra, valamint az infokommunikációs eszközök alkalmazására, szoftverfejlesztés és iratkezelés teljes folyamatára. Kiterjed továbbá valamennyi, a Társaságnál kezelt vagy feldolgozott személyes adatra, közérdekű, illetve közérdekből nyilvános adatra — függetlenül annak előállítási vagy feldolgozási módjától és megjelenési formájától — és magára az adatkezelésre, illetve adatfeldolgozásra is.

A Szabályzat hatálya mind a Rendelet, mind az Infotv. hatálya alá tartozó adatkezelésre kiterjed.

3. A Szabályzat aktualizálása

A Szabályzat aktualizálása az adatvédelmi tisztviselő javaslatára kerül végrehajtásra, melyet a következő esetekben kell kezdeményeznie:

- ha a Társaság adatvédelmét, illetve a Szabályzat tartalmát érintő jelentős változás következik be;
- ha a működtetést meghatározó jogszabályi környezetben átvezetendő változás következik be;
- a fenti eseteken túl évenként egyszer, minden év január 31. napjáig felül kell vizsgálni.

4. Fogalmak

adat
az adat tények, elképzelések, utasítások, emberi vagy technikai eszközökkel történő formalizált ábrázolása ismertetés, megőrzés, illetve feldolgozás céljára;

adatállomány
az egy nyilvántartó rendszerben kezelt adatok összessége;

adatbiztonság
az adatok jogosulatlan hozzáférés, megszerzése, módosulása, továbbítása, tönkremenetele, nyilvánosságra hozatala, illetőleg sérülés vagy a megsemmisülés, valamint a véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás elleni műszaki és szervezési megoldások rendszere;

adatfeldolgozás
az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől, feltéve hogy a technikai feladatot az adatokon végzik;

adatfeldolgozás (Infotv. szerinti adatkezelés esetén)
az adatkezelő megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által végzett adatkezelési műveletek összessége;

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

adatgazda
annak a szervezeti egységnek a vezetője, ahol mindenkori hatályos SZMSZ-ben és Ügyrendben meghatározott feladatokkal összefüggésben az adatok keletkeznek, illetve ahol az adatok jogosultságkezelése történik. A felelősségi körébe tartozó adatok vonatkozásában az adatok biztonsági osztályba sorolását elvégzi, vagy az információbiztonsági felelős által elvégzett besorolást jóváhagyja. Az adatgazdai feladatokat delegálhatja a szervezeti egysége munkavállalói részére. Az adatgazdai feladatok delegálása a külső vagy harmadik fél felé történő adatkezelési feladatokra nem terjed ki;

adathordozó
adat vagy dokumentáció és azok biztonsági másolatainak megőrzésére szolgáló
a) papír, mikrofilm, mágneses vagy egyéb elvű hagyományos, illetve

b) számítástechnikai eljárással adatokat tároló közeg
   ba) mágneses adathordozók (pl. mágnesszalag, mágneslemez, merevlemez)
   bb) optikai adathordozók (pl. CD-R/RW, DVD+/-R/RW/RAM)
   bc) egyéb elektronikus technológián alapuló tárolók (pl. ssd, flashdrive, pendrive);

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;

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;

adatkezelést végző szervezeti egység
valamennyi ügyvezető alá rendelt szervezeti egység;

adatközlő
az a közfeladatot ellátó szerv, amely – ha az adatfelelős nem maga teszi közzé az adatot – az adatfelelős által hozzá eljuttatott adatait honlapon közzéteszi;

adatmegjelölés
az adat azonosító jelzéssel ellátása annak megkülönböztetése céljából;

adatmegsemmisítés
az adatok vagy az azokat tartalmazó adathordozó teljes fizikai megsemmisítése;

adattovábbítás
ha az adatot meghatározott harmadik személy számára hozzáférhetővé teszik;

ezen belül közvetett adattovábbítás
a személyes adatnak valamely harmadik országban vagy nemzetközi szervezet keretében adatkezelést folytató adatkezelő vagy adatfeldolgozó részére továbbítása útján valamely más harmadik országban vagy nemzetközi szervezet keretében adatkezelést folytató adatkezelő vagy adatfeldolgozó részére történő továbbítása;

adattörlés
az adatok felismerhetetlenné tétele oly módon, hogy a helyreállításuk többé nem lehetséges;

adatvédelem

a személyes adatok gyűjtésének, feldolgozásának és felhasználásának korlátozását, az érintett személyek védelmét biztosító alapelvek, szabályok, eljárások, adatkezelési eszközök és módszerek összessége;

adatvédelmi tisztviselő
az az Unióban tevékenységi hellyel, illetve lakóhellyel rendelkező és az adatkezelő vagy adatfeldolgozó által írásban megjelölt természetes vagy jogi személy, aki, illetve amely az adatkezelőt vagy adatfeldolgozót képviseli az adatkezelőre vagy adatfeldolgozóra az e rendelet értelmében háruló kötelezettségek vonatkozásában;

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;

adatzárolás
az adat azonosító jelzéssel ellátása további kezelésének végleges vagy meghatározott időre történő korlátozása céljából;

álnevesítés
a személyes adatok olyan módon történő kezelése, amelynek következtében további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik, feltéve, hogy az ilyen további információt külön tárolják, és technikai és szervezési intézkedések megtételével biztosított, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet kapcsolni;

azonosító adatok
az érintett azonosítására szolgáló (személyes) adat

a) természetes azonosító adat: érintett neve, anyja neve, születési helyes és ideje, lakóhelyének ill. tartózkodási helyének címe;
b) mesterséges azonosító adat: matematikai vagy más algoritmus szerint generált adatok (pl. törzsszám, társadalombiztosítási azonosító jel (TAJ), adóazonosító jel, személyi igazolvány száma, útlevél száma);

az adatkezelés korlátozása
a tárolt személyes adatok megjelölése jövőbeli kezelésük korlátozása céljából;

az érintett hozzájárulása
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;

biztonság
az információ- és informatikai rendszerekben olyan előírások és szabványok betartását jelenti, amelyek a rendszer működőképességét, az információk rendelkezésre állását, sértetlenségét, bizalmasságát és hitelességét erősítik;

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;

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;

EGT állam
az Európai Unió tagállama és az Európai Gazdasági Térségről szóló megállapodásban részes más állam, továbbá az az állam, amelynek állampolgára az Európai Unió és tagállamai, valamint az Európai Gazdasági Térségről szóló megállapodásban nem részes állam között létrejött nemzetközi szerződés alapján az Európai Gazdasági Térségről szóló megállapodásban részes állam állampolgárával azonos jogállást élvez;

elektronikai és fotótechnikai eszköz
képi és egyéb adatok, információk rögzítésére és tárolására alkalmas eszköz (pl. analóg és digitális fényképezőgépek, kamerás mobiltelefonok);

érintett
bármely meghatározott, személyes adat alapján azonosított vagy – közvetlenül vagy közvetve – azonosítható természetes személy;

hardver
az informatikai rendszer eszközeit, fizikai elemeit alkotó részei;

harmadik fél
az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely nem azonos az érintettel, az adatkezelővel, az adatfeldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére felhatalmazást kaptak;

harmadik ország
minden olyan ország, amely nem tagja az Európai Gazdasági Térségnek;

hálózat
informatikai rendszerek összekapcsolása, amely az összekapcsolt rendszerek legkülönbözőbb komponensei között adatcserét tesz lehetővé;

információs társadalommal összefüggő szolgáltatás

az információs társadalom bármely szolgáltatása, azaz bármely, általában térítés ellenében, távolról, elektronikus úton és a szolgáltatást igénybe vevő egyéni kérelmére nyújtott szolgáltatás;

informatika
az adatok, információk elérhetőségének, rendszerezésének tudománya, amely elméletet, szemléletet és módszertant ad az információrendszerek tervezéséhez, fejlesztéséhez, szervezéséhez és működtetéséhez;

informatikai eszköz
gyűjtőnév a szoftver, hardver és adathordozó együttes meghatározására;

informatikai rendszer
a hardverek, szoftverek és adatok olyan kombinációjából álló rendszer, amit az adat-, és információfeldolgozás különböző feladatainak megoldására alkalmaznak;

irat
minden olyan szöveg, számadatsor, térkép, tervrajz és vázlat, amely valamely szerv működésével, illetőleg személy tevékenységével kapcsolatban bármilyen anyagon, alakban, bármely eszköz felhasználásával és bármely eljárással keletkezett;

iratkezelés
az irat készítését, nyilvántartását, továbbítását, rendszerezését és selejtezhetőség szempontjából történő válogatását, segédletekkel való ellátását, szakszerű és biztonságos megőrzését, használatra bocsátását, selejtezését, illetve levéltárba adását együttesen magába foglaló tevékenység;

IT-Szolgáltató
olyan gazdasági társaság, vagy természetes személy, aki érvényes szerződéses kapcsolatban áll a Társasággal és bármilyen informatikai szolgáltatás kialakításában, fejlesztésében, vagy fenntartásában vesz részt;

jogosultság
számítógépes környezetben a hozzáférési lehetőség megadása valamely tevékenység végrehajtásához;

képviselő
az az Unióban tevékenységi hellyel, illetve lakóhellyel rendelkező és az adatkezelő vagy adatfeldolgozó által a Rendelet 27. cikke alapján írásban megjelölt természetes vagy jogi személy, aki, illetve amely az adatkezelőt vagy adatfeldolgozót képviseli az adatkezelőre vagy adatfeldolgozóra az e rendelet értelmében háruló kötelezettségek vonatkozásában;

közérdekű adat
az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy 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;

közérdekből nyilvános adat
a közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli.

Közérdekből nyilvános adat a közfeladatot ellátó szerv feladat- és hatáskörében eljáró személy neve, feladatköre, munkaköre, vezetői megbízása, a közfeladat ellátásával összefüggő egyéb személyes adata, valamint azok a személyes adatai, amelyek megismerhetőségét törvény előírja. A közérdekből nyilvános személyes adatok a célhoz kötött adatkezelés elvének tiszteletben tartásával terjeszthetőek. A közérdekből nyilvános személyes adatok honlapon történő közzétételére a közfeladatot ellátó személy jogállására vonatkozó külön törvény rendelkezései irányadóak.

Ha törvény másként nem rendelkezik, közérdekből nyilvános adat a jogszabály vagy állami, illetőleg helyi önkormányzati szervvel kötött szerződés alapján kötelezően igénybe veendő vagy más módon ki nem elégíthető szolgáltatást nyújtó szervek vagy személyek kezelésében lévő, e tevékenységükre vonatkozó, személyes adatnak nem minősülő adat;

közös adatkezelő
ha az adatkezelés céljait és eszközeit két vagy több adatkezelő közösen határozza meg, azok közös adatkezelőknek minősülnek;

különleges adat

Különleges adat a személyes adatok különleges kategóriáiba tartozó minden adat, azaz a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a genetikai adatok (a Rendelet hatálya alá tartozó esetekben annak meghatározása szerint a természetes személyek egyedi azonosítását célzó genetikai adatok), a természetes személyek egyedi azonosítását célzó biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok; ezen belül:

genetikai adat: egy természetes személy örökölt vagy szerzett genetikai jellemzőire vonatkozó minden olyan személyes adat, amely az adott személy fiziológiájára vagy egészségi állapotára vonatkozó egyedi információt hordoz, és amely elsősorban az adott természetes személyből vett biológiai minta elemzéséből ered;

biometrikus adat: egy természetes személy fizikai, fiziológiai vagy viselkedési jellemzőire vonatkozó olyan, sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását, mint például az arckép vagy a daktiloszkópiai adat;

egészségügyi 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.

nemzetközi szervezet
a nemzetközi közjog hatálya alá tartozó szervezet vagy annak alárendelt szervei, vagy olyan egyéb szerv, amelyet két vagy több ország közötti megállapodás hozott létre, vagy amely ilyen megállapodás alapján jött létre;

nyilvánosságra hozatal
ha az adatot bárki számára hozzáférhetővé teszik;

profilalkotás
személyes adatok automatizált kezelésének bármely olyan formája, amelynek során a személyes adatokat valamely természetes személyhez fűződő bizonyos személyes jellemzők értékelésére, különösen a munkahelyi teljesítményhez, gazdasági helyzethez, egészségi állapothoz, személyes preferenciákhoz, érdeklődéshez, megbízhatósághoz, viselkedéshez, tartózkodási helyhez vagy mozgáshoz kapcsolódó jellemzők elemzésére vagy előrejelzésére használják;

program
eljárási leírás, amely valamely informatikai rendszer által közvetlenül vagy átalakítást követően végrehajtható;
rendkívüli adatvédelmi esemény
adatvédelmi szempontból olyan esemény, amely a Társaság információrendszerében, annak biztonságát szavatoló védelmi rendszerében súlyos károkat okoz vagy okozhat, ennek során a feladatok ellátását, a biztonságos működést veszélyezteti;

rendszer
az egymással valamilyen meghatározható kapcsolatban álló elemek összessége;

személyes adat
azonosított vagy azonosítható természetes személyre vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható;

személyes adatok határokon átnyúló adatkezelése
a) személyes adatoknak az Európai Unióban megvalósuló olyan kezelése, amelyre az egynél több tagállamban tevékenységi hellyel rendelkező adatkezelő vagy adatfeldolgozó több tagállamban található tevékenységi helyein folytatott tevékenységekkel összefüggésben kerül sor; vagy
b) személyes adatoknak az Unióban megvalósuló olyan kezelése, amelyre az adatkezelő vagy az adatfeldolgozó egyetlen tevékenységi helyén folytatott tevékenységekkel összefüggésben kerül sor úgy, hogy egynél több tagállamban jelentős mértékben érint vagy valószínűsíthetően jelentős mértékben érint érintetteket;

szoftver

számítógépen futtatható program(ok);

tiltakozás
az érintett nyilatkozata, amellyel személyes adatainak kezelését kifogásolja, és az adatkezelés megszüntetését, illetve a kezelt adatok törlését kéri;

tömeges személyes adat
a bizalmassági kategóriákba való besorolás során használt fogalom.

Ha a besorolásra kerülő adat, vagy adatcsoport – ez lehet dokumentum, táblázat, adatbázis, stb., vagy ezek csoportja – nagy mennyiségben, tömegesen tartalmaz személyes adatokat, akkor az adatot, vagy adatcsoportot a kiemelt bizalmasságú kategóriába soroljuk be.

II. FEJEZET

AZ ADATVÉDELEMRE VONATKOZÓ ÁLTALÁNOS SZABÁLYOK

1. Társaságunk, mint adatkezelő feladatai

Társaságunk az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket köteles végrehajtani annak biztosítása és bizonyítása céljából, hogy a személyes adatok kezelése a Rendelettel összhangban történik. Ezeket az intézkedéseket Társaságunk köteles felülvizsgálni és szükség esetén naprakésszé tenni.

2. Beépített és alapértelmezett adatvédelem

Társaságunk a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével mind az adatkezelés módjának meghatározásakor, mind pedig az adatkezelés során olyan megfelelő technikai és szervezési intézkedéseket – például álnevesítést – köteles végrehajtani, amelyek célja egyrészt az adatvédelmi elvek, például az adattakarékosság hatékony megvalósítása, másrészt a Rendeletben foglalt követelmények teljesítéséhez és az érintettek jogainak védelméhez szükséges garanciák beépítése az adatkezelés folyamatába.

Társaságunk megfelelő technikai és szervezési intézkedéseket köteles végrehajtani annak biztosítására, hogy alapértelmezés szerint kizárólag olyan személyes adatok kezelésére kerüljön sor, amelyek az adott konkrét adatkezelési cél szempontjából szükségesek. Ez a kötelezettség vonatkozik a gyűjtött személyes adatok mennyiségére, kezelésük mértékére, tárolásuk időtartamára és hozzáférhetőségükre. Ezek az intézkedések különösen azt kell, hogy biztosítsák, hogy a személyes adatok alapértelmezés szerint a természetes személy beavatkozása nélkül ne válhassanak hozzáférhetővé meghatározatlan számú személy számára.

3. A Társaságnál kezelt adatok osztályozása

a) *Személyes adat*

Az I. fejezet 4. pontjában meghatározottak szerint személyes adatnak minősülő adatok.

b) *Különleges adat*

Az I. fejezet 4. pontjában meghatározottak szerint különleges adatnak minősülő személyes adatok.

c) *Magántitok, levéltitok*

A Társasághoz tevékenysége során jogszerűen kerülhetnek olyan adatok, melyek a Polgári Törvénykönyvről szóló mindenkor hatályos törvény (a továbbiakban: Ptk.) alapján levéltitoknak, magántitoknak minősülnek.
Személyhez fűződő jogokat sért, aki a levéltitkot megsérti, továbbá aki a magántitok birtokába jut, és azt jogosulatlanul nyilvánosságra hozza, vagy azzal egyéb módon visszaél.

d) *Üzleti titok*

Az üzleti titok védelméről szóló 2018. évi LIV. törvényben foglalt főszabály szerint üzleti titok a gazdasági tevékenységhez kapcsolódó, titkos – egészben, vagy elemeinek összességeként nem közismert vagy az érintett gazdasági tevékenységet végző személyek számára nem könnyen hozzáférhető –, ennélfogva 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. Védett ismeret (know-how) az üzleti titoknak minősülő, azonosításra alkalmas módon rögzített, műszaki, gazdasági vagy szervezési ismeret, megoldás, tapasztalat vagy ezek összeállítása.

Nem minősül az üzleti titokhoz fűződő jog megsértésének az üzleti titok megszerzése abban az esetben, ha

- a jogosulttól független fejlesztés, felfedezés vagy alkotás,

- a nyilvánosan hozzáférhető vagy jogszerűen megszerzett termék, illetve jogszerűen igénybevett szolgáltatás vizsgálata, elemzése vagy tesztelése - feltéve, hogy az üzleti titok megszerzőjét nem terhelte az üzleti titok megszerzésére vagy megőrzésére irányuló korlátozás, különösen titoktartási kötelezettség,

- a védett ismeret körébe tartozó műszaki ismeretek és megoldások kivételével a munkavállalóknak vagy a munkavállalók képviselőinek a tájékozódáshoz és a konzultációhoz való jogának – a jogszerűen megszerzett üzleti titok munkavállaló által a munkavállalók képviselője számára történő felfedése céljából, a szükséges mértékben történő – gyakorlása,

- egyéb, a jóhiszeműség és tisztesség követelményével összeegyeztethető, az adott helyzetben általában elvárható magatartás

útján valósul meg.

Nem minősül az üzleti titokhoz fűződő jog megsértésének

- az üzleti titoknak harmadik személytől kereskedelmi forgalomban, jóhiszeműen és ellenérték fejében történő megszerzése,

- a jogszerűen megszerzett üzleti titok munkavállaló által a munkavállalók képviselője számára történő felfedése, ha a felfedés a munkavállaló vagy a képviselő tájékoztatáshoz és konzultációhoz való jogának gyakorlása céljából a jog gyakorlásához szükséges mértékben történt,

- ha az üzleti titok megszerzése, illetve az ügyben eljárni jogosult szerv számára történő felfedése jogszabálysértés vagy az üzleti tisztesség általános követelményeibe ütköző magatartás megelőzése, elkerülése, következményeinek elhárítása vagy csökkentése céljából, a közérdek védelmében, a cél által indokolt terjedelemben történik,

- ha az üzleti titok megszerzését, hasznosítását vagy felfedését közvetlenül alkalmazandó uniós jogi aktus vagy törvény írja elő, vagy teszi lehetővé.

Nem minősül üzleti titoknak az állami és a helyi önkormányzati költségvetés, illetve az európai uniós támogatás felhasználásával, költségvetést érintő juttatással, kedvezménnyel, az állami és önkormányzati vagyon kezelésével, birtoklásával, használatával, hasznosításával, az azzal való rendelkezéssel, annak megterhelésével, az ilyen vagyont érintő bármilyen jog megszerzésével kapcsolatos adat, valamint az az adat, amelynek megismerését vagy nyilvánosságra hozatalát külön törvény közérdekből elrendeli. **A nyilvánosságra hozatal azonban nem eredményezheti az olyan adatokhoz** – így különösen a védett ismerethez – **való hozzáférést, amelyek megismerése az üzleti tevékenység végzése szempontjából aránytalan sérelmet okozna, feltéve, hogy ez nem akadályozza meg a közérdekből nyilvános adat megismerésének lehetőségét.**

4. Az adatokhoz tartozó adatvédelmi, bizalmassági kategóriák

Az adatokat, adatcsoportokat jelen Szabályzat V.10. pontjában foglaltak szerint következő adatvédelmi, bizalmassági kategóriákba kell besorolni az adatkezeléshez kapcsolódó intézkedések meghatározása érdekében:

a) *Nyilvános*

Közérdekű adatok, közérdekből nyilvános adatok, valamint minden olyan további adat tartozik ebbe a kategóriába, amit a Társaság nyilvánosként sorol be.

b) *Belső*

Napi operatív munkavégzéshez szükséges, vagy az által keletkezett belső használatú adatok.

c) *Fokozott bizalmasságú*

A Társaság egyéb belső szabályozásában hozzáférés-korlátozás alá eső adatok (pl.: egyes feladatok végrehajtása érdekében bizalmas adatok), személyes adatok, valamint egyéb jogszabállyal védett titok (kivéve üzleti titok).

d) *Kiemelt bizalmasságú*

Különleges adatok, üzleti titok, valamint tömeges személyes adat.

5. Az egyes adatkezelést végző szervezeti egységek vezetőjének feladatai

Társaságunk, mint adatkezelő jelen Szabályzat hatálya alá tartozó feladatainak ellátásáért az ügyvezető alá rendelt szervezeti egység (a továbbiakban: adatkezelést végző szervezeti egység) vezetője felel.

Az adatkezelést végző szervezeti egység vezetője az irányítása alatt lévő személyektől, szervezeti egységektől megköveteli az adatvédelem, adatbiztonság szabályainak fokozott betartását és betartatását.

Felelősséget vállal az adott területen lévő adatok gyűjtéséért, az adatszolgáltatásért, az adatfeldolgozó felé történő adatszolgáltatásért.

Tevékenysége során az általa kezelt adatok vonatkozásában gondoskodik a jogszabályokban, elsősorban a Rendeletben és ezek alapján a jelen Szabályzatban meghatározott feladatok, kötelezettségek ellátásáról, különös tekintettel az érintettek jogainak védelmére, az adataik felvétele kapcsán, valamint a kérelmükre történő tájékoztatásukra, hozzájáruláson alapuló adatkezelés esetén a hozzájárulásuk beszerzésére és mindezek nyilvántartására.

Ennek megvalósítása érdekében közvetlenül az ügyvezető alá rendelt szervezeti egység vezetője köteles egy-egy olyan munkavállalót kijelölni, aki az adott szervezeti egységen belül koordinálja és az érintettek, a hatóságok, illetve harmadik személyek és szervek irányában biztosítja az adatvédelemmel kapcsolatban jelen Szabályzatban meghatározott vagy egyébként a mindenkor hatályos jogszabályok alapján felmerülő kötelezettségek teljesítését.

III. FEJEZET

A SZEMÉLYES ADATOK KEZELÉSÉRE VONATKOZÓ SZABÁLYOK

1. A személyes adatok kezelésére vonatkozó elvek

A személyes adatok:

- kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni;
- gyűjtése csak meghatározott, egyértelmű és jogszerű célból történhet, és azokat nem lehet kezelni ezekkel a célokkal össze nem egyeztethető módon (nem minősül az eredeti céllal össze nem egyeztethetőnek a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból történő további adatkezelés);
- az adatkezelés céljai szempontjából megfelelőek és relevánsak kell, hogy legyenek, és a szükségesre kell korlátozódniuk;
- pontosnak és szükség esetén naprakésznek kell lenniük; minden észszerű intézkedést meg kell tenni annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul töröljék vagy helyesbítsék;
- tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé; a személyes adatok ennél hosszabb ideig történő tárolására csak akkor kerülhet sor, amennyiben a személyes adatok kezelésére a Rendelet a 89. cikk (1) bekezdésének megfelelően közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból kerül majd sor, az érintettek jogainak és szabadságainak védelme érdekében előírt megfelelő technikai és szervezési intézkedések végrehajtására is figyelemmel;
- 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;

Az adatkezelést végző szervezeti egység vezetője felelős a fentieknek való megfelelés biztosításáéért, továbbá képesnek kell lennie e megfelelés igazolására.

A személyes adatok kezelését tisztességesnek és törvényesnek kell tekinteni, ha az érintett véleménynyilvánítási szabadságának biztosítása érdekében az érintett véleményét megismerni kívánó személy az érintett lakóhelyén vagy tartózkodási helyén felkeresi, feltéve, hogy az érintett személyes adatait e törvény rendelkezéseinek megfelelően kezelik és a személyes megkeresés nem üzleti célra irányul. A személyes megkeresésre a munka törvénykönyvéről szóló 2012. évi I. törvény (a továbbiakban: Mt.) szerinti munkaszüneti napon nem kerülhet sor.

2. A személyes adatok kezelésének feltételei

A Társaságnál személyes adat kizárólag akkor kezelhető, ha legalább az alábbiak egyike teljesül:

- az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez;

- az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél, vagy az a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges;

- az adatkezelés Társaságunkra vonatkozó hazai vagy európai uniós jogszabályon alapuló jogi kötelezettség teljesítéséhez szükséges (ez az adatkezelés kötelező adatkezelésnek minősül);

- az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges;

- az adatkezelés közérdekű vagy Társaságunkra ruházott közhatalmi jogosítvány gyakorlásának keretében végzett, hazai vagy európai uniós jogszabályon alapuló olyan feladat végrehajtásához szükséges, amely feladat csak valamely közérdekű vagy Társaságunkra ruházott közhatalmi jogosítvány gyakorlásának keretében valósítható meg (ez az adatkezelés kötelező adatkezelésnek minősül);

- az adatkezelés – érdekmérlegelési teszt alapján, melyből megállapítható, miért tekinthető arányos korlátozásnak az, hogy az adatkezelő az érintettek beleegyezése nélkül kezeljen személyes adatot – Társaságunk vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé, különösen, ha az érintett gyermek.

Kötelező adatkezelés esetén a kezelendő adatok fajtáit, az adatkezelés célját és feltételeit, az adatok megismerhetőségét, az adatkezelő személyét, valamint az adatkezelés időtartamát vagy szükségessége időszakos felülvizsgálatát az adatkezelést elrendelő törvény, illetve önkormányzati rendelet határozza meg.

Kizárólag állami vagy önkormányzati szerv kezelheti az állam bűncselekmények megelőzésére, felderítésére és üldözésére irányuló, valamint közigazgatási és igazságszolgáltatási feladatainak ellátása céljából kezelt bűnügyi személyes adatokat, valamint a szabálysértési, a polgári peres és nemperes ügyekre, valamint a közigazgatási peres és nemperes ügyekre vonatkozó adatokat tartalmazó nyilvántartásokat.

Ha a kötelező adatkezelés időtartamát vagy szükségessége időszakos felülvizsgálatát törvény, helyi önkormányzat rendelete vagy az Európai Unió kötelező jogi aktusa nem határozza meg, az adatkezelő az adatkezelés megkezdésétől legalább ötévente felülvizsgálja, hogy az általa, illetve a megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által kezelt személyes adat kezelése az adatkezelés céljának megvalósulásához szükséges-e. Ezen felülvizsgálat körülményeit és eredményét az adatkezelő dokumentálja, e dokumentációt a felülvizsgálat elvégzését követő tíz évig megőrzi és azt a Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban:

NAIH) kérésére a NAIH rendelkezésére bocsátja. A 2018. május 25-ét megelőzően megkezdett adatkezelések vonatkozásában a felülvizsgálatot 2021. május 25-ig kell elvégezni.

Bűnügyi személyes adatok kezelése esetén – ha törvény, nemzetközi szerződés vagy az Európai Unió kötelező jogi aktusa ettől eltérően nem rendelkezik – a különleges adatok kezelésének feltételeire vonatkozó szabályokat kell alkalmazni.

A tudományos kutatást végző szerv vagy személy személyes adatot nyilvánosságra hozhat, ha az a történelmi eseményekről folytatott kutatások eredményeinek bemutatásához szükséges.

Különleges adatnak minősülő személyes adat akkor kezelhető, ha legalább az alábbiak egyike teljesül:

- az érintett kifejezett hozzájárulását adta a különleges adatok egy vagy több konkrét célból történő kezeléséhez;

- az adatkezelés Társaságunknak vagy az érintettnek a foglalkoztatást, valamint a szociális biztonságot és szociális védelmet szabályozó jogi előírásokból fakadó kötelezettségei teljesítése és konkrét jogai gyakorlása érdekében szükséges, ha az érintett alapvető jogait és érdekeit védő megfelelő garanciákról is rendelkező uniós vagy tagállami jog, illetve a tagállami jog szerinti kollektív szerződés ezt lehetővé teszi;

- az adatkezelés az érintett vagy más természetes személy létfontosságú érdekeinek védelméhez szükséges, ha az érintett fizikai vagy jogi cselekvőképtelensége folytán nem képes a hozzájárulását megadni;

- az adatkezelés valamely politikai, világnézeti, vallási vagy szakszervezeti célú alapítvány, egyesület vagy bármely más nonprofit szervezet megfelelő garanciák mellett végzett jogszerű tevékenysége keretében történik, azzal a feltétellel, hogy az adatkezelés kizárólag az ilyen szerv jelenlegi vagy volt tagjaira, vagy olyan személyekre vonatkozik, akik a szervezettel rendszeres kapcsolatban állnak a szervezet céljaihoz kapcsolódóan, és hogy a személyes adatokat az érintettek hozzájárulása nélkül nem teszik hozzáférhetővé a szervezeten kívüli személyek számára;

- az adatkezelés olyan személyes adatokra vonatkozik, amelyeket az érintett kifejezetten nyilvánosságra hozott;

- az adatkezelés jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez szükséges, vagy amikor a bíróságok igazságszolgáltatási feladatkörükben járnak el;

- az adatkezelés jelentős közérdek miatt szükséges, uniós jog vagy tagállami jog alapján, amely arányos az elérni kívánt céllal, tiszteletben tartja a személyes adatok védelméhez való jog lényeges tartalmát, és az érintett alapvető jogainak és érdekeinek biztosítására megfelelő és konkrét intézkedéseket ír elő;

- az adatkezelés megelőző egészségügyi vagy munkahelyi egészségügyi célokból, a munkavállaló munkavégzési képességének felmérése, orvosi diagnózis felállítása,

egészségügyi vagy szociális ellátás vagy kezelés nyújtása, illetve egészségügyi vagy szociális rendszerek és szolgáltatások irányítása érdekében szükséges, uniós vagy tagállami jog alapján vagy egészségügyi szakemberrel kötött szerződés értelmében, ha az adatkezelés olyan szakember által vagy olyan szakember felelőssége mellett történik, aki uniós vagy tagállami jogban, illetve az arra hatáskörrel rendelkező tagállami szervek által megállapított szabályokban meghatározott szakmai titoktartási kötelezettség hatálya alatt áll, illetve olyan más személy által, aki szintén uniós vagy tagállami jogban, illetve az arra hatáskörrel rendelkező tagállami szervek által megállapított szabályokban meghatározott titoktartási kötelezettség hatálya alatt áll.

- az adatkezelés a népegészségügy területét érintő olyan közérdekből szükséges, mint a határokon át terjedő súlyos egészségügyi veszélyekkel szembeni védelem vagy az egészségügyi ellátás, a gyógyszerek és az orvostechnikai eszközök magas színvonalának és biztonságának a biztosítása, és olyan uniós vagy tagállami jog alapján történik, amely megfelelő és konkrét intézkedésekről rendelkezik az érintett jogait és szabadságait védő garanciákra, és különösen a szakmai titoktartásra vonatkozóan;

- az adatkezelés közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból szükséges olyan uniós vagy tagállami jog alapján, amely arányos az elérni kívánt céllal, tiszteletben tartja a személyes adatok védelméhez való jog lényeges tartalmát, és az érintett alapvető jogainak és érdekeinek biztosítására megfelelő és konkrét intézkedéseket ír elő.

3. A hozzájárulás feltételei

Ha az adatkezelés hozzájáruláson alapul (III. fejezet 2. pont első és hetedik francia bekezdései), az adatkezelést végző szervezeti egység vezetőjének biztosítania kell, hogy Társaságunk képes legyen annak igazolására, hogy az érintett a személyes adatainak kezeléséhez hozzájárult.

Ha az érintett hozzájárulását olyan írásbeli nyilatkozat keretében adja meg, amely más ügyekre is vonatkozik, a hozzájárulás iránti kérelmet ezektől a más ügyektől egyértelműen megkülönböztethető módon kell előadni, érthető és könnyen hozzáférhető formában, világos és egyszerű nyelvezettel. Az érintett hozzájárulását tartalmazó ilyen nyilatkozat bármely olyan része, amely sérti a Rendeletet, kötelező erővel nem bír.

Az érintett jogosult arra, hogy hozzájárulását bármikor visszavonja. A hozzájárulás visszavonása nem érinti a hozzájáruláson alapuló, a visszavonás előtti adatkezelés jogszerűségét. A hozzájárulás megadása előtt az érintettet erről tájékoztatni kell. **A hozzájárulás visszavonását ugyanolyan egyszerű módon kell lehetővé tenni, mint annak megadását.**

Annak megállapítása során, hogy a hozzájárulás önkéntes-e, a lehető legnagyobb mértékben figyelembe kell venni azt a tényt, egyebek mellett, hogy egy adott szerződés teljesítésének – beleértve a szolgáltatások nyújtását is – feltételéül szabták-e az olyan személyes adatok kezeléséhez való hozzájárulást, amelyek nem szükségesek a szerződés teljesítéséhez.

<u>A gyermek hozzájárulására vonatkozó speciális feltételek az információs társadalommal összefüggő szolgáltatások vonatkozásában:</u>

Ha az érintett hozzájárulását adta, a közvetlenül gyermekeknek kínált, információs társadalommal összefüggő szolgáltatások vonatkozásában végzett személyes adatok kezelése akkor jogszerű, ha a gyermek a 16. életévét betöltötte. A 16. életévét be nem töltött gyermek esetén, a gyermekek személyes adatainak kezelése csak akkor és olyan mértékben jogszerű, ha a hozzájárulást a gyermek feletti szülői felügyeletet gyakorló adta meg, illetve engedélyezte.

Társaságunk köteles – figyelembe véve az elérhető technológiát – észszerű erőfeszítéseket tenni azért, hogy ilyen esetekben ellenőrizze, hogy a hozzájárulást a gyermek feletti szülői felügyeleti jog gyakorlója adta meg, illetve engedélyezte.

A Társaság szervezeti egységeinél adatkezelést végző alkalmazottak kötelesek az általuk megismert személyes adatokat üzleti titokként megőrizni. Az ilyen munkakörben foglalkoztatottak számára **Titoktartási nyilatkozat (1. számú melléklet)** megtétele kötelező.

4. **A büntetőjogi felelősség megállapítására vonatkozó határozatokra és a bűncselekményekre, illetve a kapcsolódó biztonsági intézkedésekre vonatkozó személyes adatok**

Jelen pontban említett adatoknak a kezelésére kizárólag abban az esetben kerülhet sor, ha az közhatalmi szerv adatkezelésében történik, vagy ha az adatkezelést az érintett jogai és szabadságai tekintetében megfelelő garanciákat nyújtó uniós vagy tagállami jog lehetővé teszi. A büntetőjogi felelősség megállapítására vonatkozó határozatok teljes körű nyilvántartása csak közhatalmi szerv által végzett adatkezelés keretében történhet.

5. **Azonosítást nem igénylő adatkezelés**

Ha azok a célok, amelyekből Társaságunk a személyes adatokat kezeli, nem – vagy már nem – teszik szükségessé az érintettnek a Társaságunk általi azonosítását, akkor Társaságunk nem köteles kiegészítő információkat megőrizni, beszerezni vagy kezelni annak érdekében, hogy pusztán azért azonosítsa az érintettet, hogy megfeleljen a Szabályzatban foglaltaknak. Ilyen esetekben, ha bizonyítható, hogy Társaságunk nincs abban a helyzetben, hogy azonosítsa az érintettet (például azért, mert arra az adott ügytípusra vonatkozóan, amelyre az érintett kérelme vonatkozik, a megőrzési idő eltelt, ezért az ügy dokumentumai már nem állnak rendelkezésre) , az adatkezelést végző szervezeti egység vezetője köteles biztosítani, hogy erről lehetőség szerint megfelelő módon tájékoztassák az érintettet. Ilyen esetekben az érintett jogaira vonatkozó, jelen Szabályzat III. fejezet 9. a)-e) pontjai szerinti rendelkezések akkor alkalmazhatók, ha az érintett abból a célból, hogy ezen rendelkezések szerinti jogait gyakorolja, az azonosítást lehetővé tevő információt nyújt.

6. **Átlátható tájékoztatás, kommunikáció, az érintettek jogainak gyakorlására vonatkozó rendelkezések**

Az adatkezelést végző szervezeti egység vezetője köteles biztosítani, hogy az érintett részére a személyes adatok kezelésére vonatkozó valamennyi információt és jelen Szabályzat III. fejezetének vonatkozó pontjaiban rögzített minden egyes tájékoztatást tömör, átlátható, érthető és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazva nyújtsa Társaságunk, különösen a gyermekeknek címzett bármely információ esetében. Az információkat

írásban vagy más módon – ideértve adott esetben az elektronikus utat is – kell megadni. Az érintett kérésére szóbeli tájékoztatás is adható, feltéve, hogy más módon igazolták az érintett személyazonosságát.

Az adatkezelést végző szervezeti egység vezetője köteles gondoskodni arról, hogy Társaságunk elősegítse az érintett jelen Szabályzat III. fejezete szerinti jogainak a gyakorlását. Azonosítást nem igénylő adatkezelés esetekben Társaságunk az érintett jogai gyakorlására irányuló kérelmének a teljesítését nem tagadhatja meg, kivéve, ha bizonyítja, hogy az érintettet nem áll módjában azonosítani.

Az adatkezelést végző szervezeti egység vezetője köteles biztosítani, hogy **indokolatlan késedelem nélkül, de mindenféleképpen a kérelem beérkezésétől számított egy hónapon belül tájékoztassa az érintettet a jelen Szabályzat III. fejezete szerinti kérelem nyomán hozott intézkedésekről. Szükség esetén, figyelembe véve a kérelem összetettségét és a kérelmek számát, ez a határidő további két hónappal meghosszabbítható. A határidő meghosszabbításáról a késedelem okainak megjelölésével a kérelem kézhezvételétől számított egy hónapon belül kell tájékoztatni az érintettet**. Ha az érintett elektronikus úton nyújtotta be a kérelmet, a tájékoztatást lehetőség szerint elektronikus úton kell megadni, kivéve, ha az érintett azt másként kéri.

Ha Társaságunk nem tesz intézkedéseket az érintett kérelme nyomán, késedelem nélkül, de legkésőbb a kérelem beérkezésétől számított egy hónapon belül tájékoztatni kell az érintettet az intézkedés elmaradásának okairól, valamint arról, hogy az érintett panaszt nyújthat be valamely felügyeleti hatóságnál, és élhet bírósági jogorvoslati jogával.

A fentiek szerinti információkat, tájékoztatást díjmentesen kell biztosítani. Ha az érintett kérelme egyértelműen megalapozatlan vagy – különösen ismétlődő jellege miatt – túlzó, Társaságunk, figyelemmel a kért információ vagy tájékoztatás nyújtásával vagy a kért intézkedés meghozatalával járó adminisztratív költségekre:

a) észszerű összegű díjat számíthat fel, vagy

b) megtagadhatja a kérelem alapján történő intézkedést.

A kérelem egyértelműen megalapozatlan vagy túlzó jellegének bizonyítása Társaságunkat terheli. Amennyiben megalapozott kétség áll fenn a fentiek szerinti kérelmet benyújtó természetes személy kilétével kapcsolatban, további, az érintett személyazonosságának megerősítéséhez szükséges információk nyújtása kérhető.

Az érintett részére nyújtandó információkat szabványosított ikonokkal is ki lehet egészíteni annak érdekében, hogy a tervezett adatkezelésről az érintett jól látható, könnyen érthető és jól olvasható formában kapjon általános tájékoztatást. Az elektronikusan megjelenített ikonoknak géppel olvashatónak kell lenniük.

7. Tájékoztatás és a személyes adatokhoz való hozzáférés

7.1. Az érintettek rendelkezésére bocsátandó információk, ha a személyes adatokat az érintettől gyűjtik

Ha az érintettre vonatkozó személyes adatok magától az érintettől kerülnek Társaságunk birtokába, az adatkezelést végző szervezeti egység vezetője köteles gondoskodni arról, hogy a személyes adatok megszerzésének időpontjában Társaságunk az érintett rendelkezésére bocsássa – az adatkezelések nyilvántartásában (VIII. fejezet) szereplő információk alapul vételével – a következő információk mindegyikét:

- Társaságunk elérhetőségei;
- az adatvédelmi tisztviselő munkahelyi elérhetőségei;
- a személyes adatok tervezett kezelésének célja, valamint az adatkezelés jogalapja;
- ha az adatkezelés az érintett vagy egy másik természetes személy jogos érdekeinek védelme miatt szükséges, Társaságunk vagy harmadik fél jogos érdekei;
- adott esetben a személyes adatok címzettjei, illetve a címzettek kategóriái, ha van ilyen;
- adott esetben annak ténye, hogy Társaságunk harmadik országba vagy nemzetközi szervezet részére kívánja továbbítani a személyes adatokat, kiegészítve a Rendelet 13. cikk (1) bekezdés f) pontja szerinti információkkal.

A fenti információk mellett Társaságunk a személyes adatok megszerzésének időpontjában, annak érdekében, hogy a tisztességes és átlátható adatkezelést biztosítsa, az érintettet a következő kiegészítő információkról tájékoztatja:

a) a személyes adatok tárolásának időtartamáról, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjairól;

b) az érintett azon jogáról, hogy kérelmezheti Társaságunktól a rá vonatkozó személyes adatokhoz való hozzáférést, azok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen, valamint az érintett adathordozhatósághoz való jogáról;

c) az érintett hozzájárulásán alapuló adatkezelés esetén a hozzájárulás bármely időpontban történő visszavonásához való jog, amely nem érinti a visszavonás előtt a hozzájárulás alapján végrehajtott adatkezelés jogszerűségét;

d) a felügyeleti hatósághoz címzett panasz benyújtásának jogáról;

e) arról, hogy a személyes adat szolgáltatása jogszabályon vagy szerződéses kötelezettségen alapul vagy szerződés kötésének előfeltétele-e, valamint hogy az érintett köteles-e a személyes adatokat megadni, továbbá hogy milyen lehetséges következményeikkel járhat az adatszolgáltatás elmaradása;

f) ha indokolt, az automatizált döntéshozatal tényéről, ideértve a profilalkotást is, valamint – legalább ezekben az esetekben – az alkalmazott logikára és arra vonatkozóan érthető információk, hogy az ilyen adatkezelés milyen jelentőséggel, és az érintettre nézve milyen várható következményekkel bír.

Ha Társaságunk a személyes adatokon a gyűjtésük céljától eltérő okból további adatkezelést kíván végezni, a további adatkezelést megelőzően tájékoztatnia kell az érintettet erről az eltérő okról és a fent említett minden releváns kiegészítő információról.

Fenti rendelkezések nem alkalmazandók, ha az érintett már rendelkezik az információkkal.

7.2. Az érintettek rendelkezésére bocsátandó információk, ha a személyes adatokat nem az érintettől szerezték meg

Ha a személyes adatok nem az érintettől jutnak el Társaságunkhoz, az adatkezelést végző szervezeti egység vezetője köteles gondoskodni arról, hogy Társaságunk az érintett rendelkezésére bocsássa a fenti 7.1. pontba foglaltakon túl a következő információkat is:

- az érintett személyes adatok kategóriái;
- a személyes adatok forrása és adott esetben az, hogy az adatok nyilvánosan hozzáférhető forrásokból származnak-e.

Fenti információkat az alábbiak szerint kell megadni:

a) a személyes adatok kezelésének konkrét körülményeit figyelembe véve, a személyes adatok megszerzésétől számított észszerű határidőn, de legkésőbb egy hónapon belül;

b) ha a személyes adatokat az érintettel való kapcsolattartás céljára használják, legalább az érintettel való első kapcsolatfelvétel alkalmával; vagy

c) ha várhatóan más címzettel is közlik az adatokat, legkésőbb a személyes adatok első alkalommal való közlésekor.

Ha Társaságunk a személyes adatokon a megszerzésük céljától eltérő okból további adatkezelést kíván végezni, a további adatkezelést megelőzően tájékoztatnia kell az érintettet erről az eltérő okról és az egyéb releváns kiegészítő információról.

Jelen 7.2 pont a), b), és c) bekezdéseit, valamint a fenti bekezdést nem kell alkalmazni, ha és amilyen mértékben:

a) az érintett már rendelkezik az információkkal;

b) a szóban forgó információk rendelkezésre bocsátása lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényelne, különösen a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból folytatott adatkezelésre vonatkozó, a Rendelet 89. § (1) bekezdése szerinti feltételek és garanciák figyelembevételével végzett adatkezelés esetében, vagy amennyiben jelen 7.2 pontban

említett kötelezettség valószínűsíthetően lehetetlenné tenné vagy komolyan veszélyeztetné ezen adatkezelés céljainak elérését. Ilyen esetekben Társaságunknak megfelelő intézkedéseket kell hoznia – az információk nyilvánosan elérhetővé tételét is ideértve – az érintett jogainak, szabadságainak és jogos érdekeinek védelme érdekében;

c) az adat megszerzését vagy közlését kifejezetten előírja a Társaságunkra irányadó uniós vagy tagállami jog, amely az érintett jogos érdekeinek védelmét szolgáló megfelelő intézkedésekről rendelkezik; vagy

d) a személyes adatoknak valamely uniós vagy tagállami jogban előírt szakmai titoktartási kötelezettség alapján, ideértve a jogszabályon alapuló titoktartási kötelezettséget is, bizalmasnak kell maradnia.

8. Egyes kiemelt személyes adatkezelések társasági szabályai

a) *Munkaviszony létesítése, módosítása, megszűnése kapcsán történő adatkezelés*

Az Mt., a foglalkoztatás elősegítéséről, a munkanélküliek ellátásáról szóló 1991. évi IV. törvény, valamint az adózás rendjéről szóló 2017. évi CL. törvény rendelkezik a Társaság által nyilvántartható adatok köréről. Az Mt. meghatározza, hogy a munkavállalótól olyan nyilatkozat megtétele vagy személyes adat közlése követelhető, amely a munkaviszony létesítése, teljesítése, megszűnése (megszüntetése) vagy az Mt.-ből származó igény érvényesítése szempontjából lényeges, továbbá ebben a körben okirat bemutatása követelhető. Felhatalmazást ad a munkaidővel és szabadságolással kapcsolatos adatok kezelésére is.

A **munkaszerződésben** fel kell tüntetni azokat a természetes személyazonosító adatokat (név, anyja neve, születési hely és idő), lakcímet, melyek a munkavállaló egyértelmű azonosításához szükségesek. A Társaság további személyes adatokat kötelező adatkezelés keretében kezel (pl. a munkavállaló tartózkodási helyét, levelezési címét, adóazonosító jelét, társadalombiztosítási azonosító számát, iskolai és szakképzettséget igazoló bizonyítványok adatait, stb.), mivel bejelentési, bevallási, illetve különböző fizetési kötelezettségeinek a Társaság csak így tud eleget tenni.

A Társaság **a munkaviszony megszüntetésekor (megszűnésekor)** a munkavállaló részére az alábbiakban meghatározott tartalmú igazolást állít ki. Az igazolás tartalmazza:

- a munkavállaló személyi adatait (név, születéskori név, anyja születéskori neve, születési hely és idő, adóazonosító jel, TAJ szám, lakcím),
- a munkáltatónál munkaviszonyban töltött idő tartamát, munkakörét,
- a munkavállaló munkabéréből jogerős határozat vagy jogszabály alapján levonandó tartozást, illetve ennek jogosultját,
- a munkavállaló által a munkaviszony megszűnésének évében igénybe vett betegszabadság időtartamát,
- a munkavállaló végkielégítésben való részesülését,
- a munkáltató köteles igazolni azt is, ha a munkavállaló munkabérét tartozás nem terheli,
- az igazolásnak tartalmaznia kell a munkavállaló pénztártag által választott magánnyugdíj-pénztár megnevezését, címét, bankszámlaszámát; ha a tagságra kötelezett pályakezdő

munkavállaló nem választott pénztárat, ezt a tényt jelezni kell, és meg kell jelölni az illetékes területi pénztár megnevezését, címét.

A munkavállaló, ha a munkaviszony legalább egy évig fennállt, a munkaviszony megszüntetésekor (megszűnésekor) vagy legfeljebb az ezt követő egy éven belül munkájáról írásban értékelést kérhet.

b) *Munkabér, egyéb járandóság, illetőleg a munkaviszony kapcsán keletkező egyéb adatok kezelése*

Minden személy munkabérére és egyéb járandóságára, továbbá a munkaviszony kapcsán keletkező egyéb adatok (tisztség vagy munkakör, munkaviszonyban álló személy esetében a munkavállaló részére a munkaviszonya alapján közvetlenül vagy közvetve nyújtott pénzbeli juttatások (alapbér, egyéb időbér, teljesítménybér, valamint az időbért megalapozó időtartam, illetve a teljesítménybért megalapozó teljesítménykövetelmények), a munkavállalóra irányadó végkielégítés, illetve felmondási idő időtartama, az Mt. 228. §-ban szabályozott versenytilalmi megállapodás alapján kikötött időtartam és a kötelezettség vállalásának ellenértéke, a Ptk. 3:112. §-a szerinti jogviszony (társasági jogi jogviszony a Ptk. megbízásra vonatkozó szabályai alapján), valamint a felügyelőbizottsági tagok esetén a megbízási díj, a megbízási díjon felüli egyéb járandóságok, a jogviszony megszűnése esetén járó pénzbeli juttatások) kezelése során annak nyilvánosságra hozatala, illetéktelen személy tudomására hozatala tilos, kivéve az Infotv.-ben a közérdekű és közérdekből nyilvános adatok közzétételére vonatkozó kötelezettséget, valamint a köztulajdonban álló gazdasági társaságok takarékosabb működéséről szóló 2009. évi CXXII. törvényben (a továbbiakban: Közzétételi tv), továbbá a mindenkor hatályos Közzétételi Szabályzatban foglalt munkaköröket, illetőleg azon adatköröket, melyek közérdekből nyilvános adatnak minősülnek.

A munkabérről, munkaviszonnyal kapcsolatos egyéb személyes adatról (pl. szabadság-nyilvántartás, munkakör stb.) adott tájékoztató kimutatást (pl. bérnapló) úgy kell az érintetthez eljuttatni, hogy az abban foglalt adatok illetéktelenek számára ne legyenek hozzáférhetőek.

c) *Videómegfigyelő-rendszerek működtetése*

A Társaság által működtetett videómegfigyelő-rendszerek üzemeltetése során az alábbiakat kell figyelembe venni:
A kamerákat jól látható helyekre kell felszerelni, és a rögzített felvételeket a lentiekben meghatározott idő elteltével törölni kell.

C.1. A munkavégzésre szolgáló helyen az alábbiak szerint kell eljárni (a Rendelet, illetve az Mt. alapján):

Alkalmazható videómegfigyelő-rendszer az emberi élet, testi épség, személyi szabadság védelme, a veszélyes anyagok őrzése, az üzleti, fizetési, bank- és értékpapírtitok védelme, valamint vagyonvédelem érdekében, továbbá munkáltatói ellenőrzés céljából, amennyiben az a munkaviszony rendeltetésével közvetlenül összefüggő okból feltétlenül szükséges, és nem célja a munkavállaló munkahelyi viselkedésének a befolyásolása.

A munkáltatói ellenőrzés és az annak során alkalmazott eszközök, módszerek nem járhatnak az emberi méltóság megsértésével, így például öltözőben, próbafülkében, mosdóban, illemhelyen, a munkaközi szünet eltöltésére kijelölt helyen, dohányzóban tilos a megfigyelés, továbbá a munkavállaló magánélete nem ellenőrizhető.

Videómegfigyelő-rendszer kizárólag magánterületen alkalmazható.

A munkavállalót előzetesen tájékoztatni kell az adatkezelés lényeges követelményeiről.

A megfigyelt területen jól látható helyen, piktogrammal jelezni kell a kamerás megfigyelés tényét, illetőleg a piktogram alatt az alábbi szöveget kell elhelyezni:

„Figyelem! Videómegfigyelő-rendszerrel ellátott terület.

Az Európai Parlament és a Tanács 2016. április 27-i (EU) 2016/679. számú, 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 rendeletének (a továbbiakban: Rendelet) 6. cikk (1) bekezdés f) pontja alapján a BKV Zrt. vagyontárgyainak védelme érdekében elektronikus biztonságtechnikai rendszer által megfigyelést és adatrögzítést végez. Az adatok tárolása a felhasználás hiányában legfeljebb a rögzítéstől számított 3 munkanap, illetve a Társasági Adatvédelmi és Adatbiztonsági Szabályzatban meghatározott esetekben 30 nap időtartamban történik. Az érintettek jogaira a Rendelet III. fejezetének rendelkezései irányadók.

BKV Panoráma Kft.”

A fentieken túl a kamerás megfigyeléssel érintett területeken munkát végző munkavállalónak írásbeli tájékoztatást kell átadni, vagy őket dokumentált módon kell tájékoztatni, amelynek ki kell terjednie:
• az adatkezelés jogalapjára[1],
• az egyes kamerák elhelyezésére és a vonatkozásukban fennálló célra, az általuk megfigyelt területre, tárgyra, illetőleg arra, hogy az adott kamerával közvetlen vagy rögzített megfigyelést végez-e a munkáltató,[2]
• az elektronikus megfigyelőrendszert üzemeltető (jogi vagy természetes) személy meghatározására,[3]
• a felvétel tárolásának helyére és időtartamára,[4]

1 Jelen Szabályzat III.2. pontja alapulvételével

2 Területileg eltérő lehet (pl.: a xxx területen található kamera elhelyezésének a célja a társasági vagyon védelme/veszélyes anyagok védelme stb., a kamerával a munkáltató rögzítést nem, csak közvetlen megfigyelést folytat)

3 Területileg eltérő lehet, de jellemzően: BKV Zrt. vagy BKV Panoráma Kft.

4 A lentiek szerint az időtartam vonatkozásában (tehát 3 munkanap, vagy 30 nap, az adatrögzítés céljától függően)

• a felvételek tárolásával kapcsolatos adatbiztonsági intézkedésekre,[5]
• az adatok megismerésére jogosult személyek körére, illetőleg arra, hogy a felvételeket mely személyek, szervek részére, milyen esetben továbbíthatja,[6]
• a felvételek visszanézésére vonatkozó szabályokra, illetőleg arra, hogy a felvételeket milyen célból használhatja fel a munkáltató,[7]
• arra, hogy a munkavállalókat milyen jogok illetik meg az elektronikus megfigyelőrendszerrel összefüggésben és milyen módon tudják gyakorolni a jogaikat,[8]
• arra, hogy az információs önrendelkezési joguk megsértése esetén milyen jogérvényesítési eszközöket vehetnek igénybe.[9]

A fenti kérdések vonatkozásában a videómegfigyelő-rendszert alkalmazó az adatkezelést végző szervezeti egységek érintett szakterületeinek terület-specifikus szabályozást kell kialakítaniuk, az adatvédelmi tisztviselővel egyeztetniük, és azt a munkavállalók részére kimutathatóan oktatni kell.

A felvételek megőrzése – felhasználás hiányában – legfeljebb 3 munkanapnyi időtartamra lehetséges. A rögzített kép-, hang, valamint kép- és hangfelvételt felhasználás hiányában legfeljebb a rögzítéstől számított harminc nap elteltével kell megsemmisíteni, illetve törölni, ha a rögzítésre nyilvános rendezvényen az emberi élet, testi épség, személyi szabadság védelme, nyilvános rendezvényen, közforgalmú közlekedési eszköz állomásán, megállóhelyén (pl. vasútállomáson, metrómegállóban) terrorcselekmény és közveszélyokozás megelőzése, a Büntető Törvénykönyvről szóló törvény szerint legalább jelentős értékű pénz, értékpapír, nemesfém, drágakő biztonságos tárolása, kezelése, szállítása, vagy veszélyes anyagok őrzése érdekében kerül sor.

Az, akinek jogát vagy jogos érdekét a kép-, hang-, vagy a kép- és hangfelvétel, illetve más személyes adatának rögzítése érinti, a kép-, hang-, valamint kép- és hangfelvétel, illetve más személyes adat rögzítésétől számított három munkanapon, illetőleg a fentiek szerint 30 napos határidő esetén 30 napon belül jogának vagy jogos érdekének igazolásával kérheti, hogy az adatot annak kezelője ne semmisítse meg, illetve ne törölje. Az érdek/jog egyidejű igazolása mellett kezdeményezett felvétel megőrzési kérelemnek köteles a munkáltató eleget tenni, továbbá az érintett részére kérésére a rögzített felvételekhez hozzáférést, betekintést engedni, a felvételekről részére másolatot kiadni.

[5] Területileg eltérő lehet (pl.: „Az adatok egyirányú kódolási algoritmus (hash-kód) alkalmazásával kerülnek továbbításra és az adatkezelőknél a biztonsági adategyeztetéshez kapcsolódóan nem rögzít személyes adatokat.” Vagy: „Az adatkezelő az adattovábbítás jogszerűségének ellenőrzése, valamint az érintett tájékoztatása céljából adattovábbítási nyilvántartást vezet, amely tartalmazza az általa kezelt személyes adatok továbbításának időpontját, az adattovábbítás jogalapját és címzettjét, a továbbított személyes adatok körének meghatározását, valamint az adatkezelést előíró jogszabályban meghatározott egyéb adatokat.”)

[6] Területileg eltérő lehet

[7] Jelen Szabályzatban meghatározott alapelvek szem előtt tartásával, az adatvédelmi tisztviselővel egyeztetve

[8] Jelen Szabályzat III.9. pontjában foglaltak megfelelő alkalmazásával

[9] Rendelet 58. cikk; Infotv. 22. §, és 52. §

A fentiekből következően, amennyiben a megfigyelés célja pl. veszélyes anyagok őrzése, úgy a 30 napos időtartamot, amennyiben pl. az emberi élet védelme a cél, de nem nyilvános rendezvényen, úgy 3 munkanapos határidőt kell figyelembe venni.

Bíróság vagy más hatóság megkeresésére a rögzített kép-, hang-, valamint kép- és hangfelvételt, valamint más személyes adatot a bíróságnak vagy a hatóságnak haladéktalanul meg kell küldeni. Amennyiben megkeresésre attól számított 30 napon belül, hogy a megsemmisítés mellőzését kérték, nem kerül sor, a rögzített kép-, hang-, valamint kép- és hangfelvételt, valamint más személyes adatot meg kell semmisíteni, illetve törölni kell.

Az adatokat megismerheti továbbá azon munkavállaló, akinek feladata az adatkezelés céljának megvalósítása, illetve annak elősegítése. A felvételek visszanézésének rendjét az adatkezelést végző szervezeti egységek érintett szakterületeinek egyedileg kell kialakítaniuk, a szabályozást annak kiadása előtt az adatvédelmi tisztviselővel egyeztetni kell.

d) *Társasági testületi üléseken, érdekképviseleti egyeztetéseken történő hangrögzítés*

Amennyiben az igazgatósági és felügyelőbizottsági üléseken, érdekképviseleti szervekkel történő egyeztetéseken elhangzottak kép-, hang-, kép -és hangfelvételen történő rögzítésére kerül sor, az adatkezelés jogalapja a Társaságnak, illetve az egyeztetésen jelenlévők által képviselt szervezeteknek az elhangzottak alátámaszthatóságához, megfelelő, valósághű írásban történő dokumentálásához fűződő jogos érdeke.

Ebben a körben az igazgatósági és felügyelőbizottsági tagok, érdekképviseletek nevében eljáró személyek, munkavállalók, illetve egyéb meghívottak személyes adatainak kezelése történhet.
A felvételeket az adatkezelés céljával összefüggésben a felvétel készítésében, illetve az annak alapján történő dokumentálásban közreműködő munkavállalók ismerhetik meg.

Az adatok törlésére előirányzott határidő az adott egyeztetéshez kapcsolódóan a jogszabályban biztosított bírósági jogorvoslati határidő elteltét követő 30. nap. Ez igazgatósági és felügyelőbizottsági üléseken történő rögzítés esetén a határozat meghozatalát követő naptól számított 60. nap, érdekképviseleti szervekkel történő egyeztetések rögzítése esetén az egyeztetés lezárását követő 35. nap.

9. Érintettek jogai és érvényesítésük

a) *Tájékoztatásra, illetve betekintésre irányuló kérelem*

Az érintett jogosult arra, hogy jelen Szabályzat III. 6. pontja szerinti felelős útján, eljárási rendben és határidőkkel Társaságunktól visszajelzést kapjon arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e, és ha ilyen adatkezelés folyamatban van, jogosult arra, hogy a személyes adatokhoz és a következő információkhoz hozzáférést kapjon:

a) az adatkezelés céljai;
b) az érintett személyes adatok kategóriái;

c) azon címzettek vagy címzettek kategóriái, akikkel, illetve amelyekkel a személyes adatokat közölték vagy közölni fogják, ideértve különösen a harmadik országbeli címzetteket, illetve a nemzetközi szervezeteket;
d) adott esetben a személyes adatok tárolásának tervezett időtartama, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjai;
e) az érintett azon joga, hogy kérelmezheti az adatkezelőtől a rá vonatkozó személyes adatok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen;
f) a valamely felügyeleti hatósághoz címzett panasz benyújtásának joga;
g) ha az adatokat nem az érintettől gyűjtötték, a forrásukra vonatkozó minden elérhető információ;
h) a Rendelet 22. cikk (1) és (4) bekezdése szerinti automatizált döntéshozatal ténye, ideértve a profilalkotást is, valamint legalább ezekben az esetekben az alkalmazott logikára és arra vonatkozó érthető információk, hogy az ilyen adatkezelés milyen jelentőséggel bír, és az érintettre nézve milyen várható következményekkel jár.

Ha személyes adatoknak harmadik országba vagy nemzetközi szervezet részére történő továbbítására kerül sor, az érintett jogosult arra, hogy tájékoztatást kapjon a továbbításra vonatkozóan a Rendelet 46. cikke szerinti megfelelő garanciákról.

Társaságunk az adatkezelés tárgyát képező személyes adatok másolatát az érintett rendelkezésére bocsátja. Az érintett által kért további másolatokért Társaságunk az adminisztratív költségeken alapuló, észszerű mértékű díjat számíthat fel. Ha az érintett elektronikus úton nyújtotta be a kérelmet, az információkat széles körben használt elektronikus formátumban kell rendelkezésre bocsátani, kivéve, ha az érintett másként kéri. A másolat igénylésére vonatkozó jog nem érintheti hátrányosan mások jogait és szabadságait.

b) *Helyesbítéshez való jog*

Az érintett jogosult arra, hogy kérésére Társaságunk indokolatlan késedelem nélkül helyesbítse a rá vonatkozó pontatlan személyes adatokat. Figyelembe véve az adatkezelés célját, az érintett jogosult arra, hogy kérje a hiányos személyes adatok – egyebek mellett kiegészítő nyilatkozat útján történő – kiegészítését.

c) *Törléshez való jog*

Az érintett jogosult arra, hogy kérésére Társaságunk indokolatlan késedelem nélkül törölje a rá vonatkozó személyes adatokat, Társaságunk pedig köteles arra, hogy az érintettre vonatkozó személyes adatokat indokolatlan késedelem nélkül törölje, ha az alábbi indokok valamelyike fennáll:

a) a személyes adatokra már nincs szükség abból a célból, amelyből azokat gyűjtötték vagy más módon kezelték;
b) az érintett visszavonja az adatkezelés alapját képező hozzájárulását, és az adatkezelésnek nincs más jogalapja;
c) az érintett tiltakozik az adatkezelése ellen, és nincs elsőbbséget élvező jogszerű ok az adatkezelésre;

d) a személyes adatokat jogellenesen kezelték;
e) a személyes adatokat a Társaságunkra alkalmazandó uniós vagy tagállami jogban előírt jogi kötelezettség teljesítéséhez törölni kell;
f) a személyes adatok gyűjtésére információs társadalommal összefüggő szolgáltatások kínálásával kapcsolatosan került sor.

Ha Társaságunk nyilvánosságra hozta a személyes adatot, és az előzőek értelmében azt törölni köteles, az elérhető technológia és a megvalósítás költségeinek figyelembevételével megteszi az észszerűen elvárható lépéseket – ideértve technikai intézkedéseket – annak érdekében, hogy tájékoztassa az adatokat kezelő adatkezelőket, hogy az érintett kérelmezte tőlük a szóban forgó személyes adatokra mutató linkek vagy e személyes adatok másolatának, illetve másodpéldányának törlését.

A személyes adatokat a fentiektől eltérően nem kell törölni, amennyiben az adatkezelés szükséges
- a véleménynyilvánítás szabadságához és a tájékozódáshoz való jog gyakorlása céljából;
- a személyes adatok kezelését előíró, Társaságunkra alkalmazandó uniós vagy tagállami jog szerinti kötelezettség teljesítése, illetve közérdekből vagy Társaságunkra ruházott közhatalmi jogosítvány gyakorlása keretében végzett feladat végrehajtása céljából;
- népegészségügy területét érintő közérdek alapján, jelen Szabályzat III. 2 pontjában a különleges adatok kezelésére vonatkozóan a 8. és 9. bekezdésben meghatározottak szerint;
- a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból, amennyiben a törlés valószínűsíthetően lehetetlenné tenné vagy komolyan veszélyeztetné ezt az adatkezelést; vagy
- jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez.

d) *Az adatkezelés korlátozásához való jog*

Az érintett jogosult arra, hogy kérésére Társaságunk korlátozza az adatkezelést, ha az alábbiak valamelyike teljesül:

a) az érintett vitatja a személyes adatok pontosságát, ez esetben a korlátozás arra az időtartamra vonatkozik, amely lehetővé teszi, hogy Társaságunk ellenőrizze a személyes adatok pontosságát;
b) az adatkezelés jogellenes, és az érintett ellenzi az adatok törlését, és ehelyett kéri azok felhasználásának korlátozását;
c) Társaságunknak már nincs szüksége a személyes adatokra adatkezelés céljából, de az érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez; vagy
d) az érintett tiltakozott az adatkezelés ellen, ez esetben a korlátozás arra az időtartamra vonatkozik, amíg megállapításra nem kerül, hogy a Társaságunk jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben.

Ha az adatkezelés a fentiek szerint korlátozás alá esik, az ilyen személyes adatokat a tárolás kivételével csak az érintett hozzájárulásával, vagy jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez, vagy más természetes vagy jogi személy jogainak védelme érdekében, vagy az Unió, illetve valamely tagállam fontos közérdekéből lehet kezelni.

Társaságunk az érintettet, akinek a kérésére fentiek alapján korlátozták az adatkezelést, az adatkezelés korlátozásának feloldásáról előzetesen tájékoztatja.

Jelen 9. pont b), c), d), pontjaiban rögzített jogok érvényesítése esetén Társaságunk minden olyan címzettet a fentiek szerinti intézkedésről, akivel, illetve amellyel a személyes adatot közölték, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel. Az érintettet kérésére Társaságunk tájékoztatja e címzettekről.

e) *Az adathordozhatósághoz való jog*

Az érintett jogosult arra, hogy a rá vonatkozó, általa egy adatkezelő rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja, továbbá jogosult arra, hogy ezeket az adatokat egy másik adatkezelőnek továbbítsa anélkül, hogy ezt akadályozná Társaságunk, amelynek a személyes adatokat a rendelkezésére bocsátotta, ha:

- az adatkezelés hozzájáruláson, vagy szerződésen alapul; és
- az adatkezelés automatizált módon történik.

Az adatok hordozhatóságához való jog e fejezet szerinti gyakorlása során az érintett jogosult arra, hogy – ha ez technikailag megvalósítható – kérje a személyes adatok adatkezelők közötti közvetlen továbbítását és ezen jog gyakorlása nem sértheti a törléshez való jogát az érintettnek. Az említett jog nem alkalmazandó abban az esetben, ha az adatkezelés közérdekű vagy Társaságunkra ruházott közhatalmi jogosítványai gyakorlásának keretében végzett feladat végrehajtásához szükséges. Az adathordozhatósághoz való jog nem érintheti hátrányosan mások jogait és szabadságait.

f) *Tiltakozáshoz való jog*

Az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okból bármikor tiltakozzon a közérdeken vagy Társaságunkra ruházott közhatalmi jogosítványon alapuló, illetve a jogos érdeken alapuló személyes adatkezelése ellen, ideértve az említett rendelkezéseken alapuló profilalkotást is. Ebben az esetben Társaságunk a személyes adatokat nem kezelheti tovább, kivéve, ha Társaságunk bizonyítja, hogy az adatkezelést olyan kényszerítő erejű jogos okok indokolják, amelyek elsőbbséget élveznek az érintett érdekeivel, jogaival és szabadságaival szemben, vagy amelyek jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódnak.

Ha a személyes adatok kezelése közvetlen üzletszerzés érdekében történik, az érintett jogosult arra, hogy bármikor tiltakozzon a rá vonatkozó személyes adatok e célból történő kezelése ellen, ideértve a profilalkotást is, amennyiben az a közvetlen üzletszerzéshez kapcsolódik.

Ha az érintett tiltakozik a személyes adatok közvetlen üzletszerzés érdekében történő kezelése ellen, akkor a személyes adatok a továbbiakban e célból nem kezelhetők.

Jelen pontban említett jogra legkésőbb az érintettel való első kapcsolatfelvétel során kifejezetten fel kell hívni annak figyelmét, és az erre vonatkozó tájékoztatást egyértelműen és minden más információtól elkülönítve kell megjeleníteni.

Az információs társadalommal összefüggő szolgáltatások igénybevételéhez kapcsolódóan és a 2002/58/EK. irányelvtől eltérve az érintett a tiltakozáshoz való jogot műszaki előírásokon alapuló automatizált eszközökkel is gyakorolhatja.

Ha a személyes adatok kezelésére tudományos és történelmi kutatási célból vagy statisztikai célból kerül sor, az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból tiltakozhasson a rá vonatkozó személyes adatok kezelése ellen, kivéve, ha az adatkezelésre közérdekű okból végzett feladat végrehajtása érdekében van szükség.

g) *Automatizált döntéshozatal egyedi ügyekben, beleértve a profilalkotást*

Az érintett jogosult arra, hogy ne terjedjen ki rá az olyan, kizárólag automatizált adatkezelésen – ideértve a profilalkotást is (melynek definíciója megtalálható az I. fejezet 4. pontjában), – alapuló döntés hatálya, amely rá nézve joghatással járna vagy őt hasonlóképpen jelentős mértékben érintené.

Fenti jogosultság nem alkalmazandó abban az esetben, ha a döntés:

a) az érintett és Társaságunk közötti szerződés megkötése vagy teljesítése érdekében szükséges;
b) meghozatalát Társaságunkra alkalmazandó olyan uniós vagy tagállami jog teszi lehetővé, amely az érintett jogainak és szabadságainak, valamint jogos érdekeinek védelmét szolgáló megfelelő intézkedéseket is megállapít; vagy
c) az érintett kifejezett hozzájárulásán alapul.

Az a) és c) alpontjaiban említett esetekben Társaságunk köteles megfelelő intézkedéseket tenni az érintett jogainak, szabadságainak és jogos érdekeinek védelme érdekében, ideértve az érintettnek legalább azt a jogát, hogy Társaságunk részéről emberi beavatkozást kérjen, álláspontját kifejezze, és a döntéssel szemben kifogást nyújtson be.
Jelen pont második bekezdés a)-c) pontja szerinti döntések nem alapulhatnak a személyes adatoknak a II. fejezet 3. pont b) pontban rögzített különleges kategóriáin, kivéve, ha az adatkezelés hozzájáruláson alapul vagy jelentős közérdekből szükséges az adatkezelés uniós vagy tagállamijog alapján, és az érintett jogainak, szabadságainak és jogos érdekeinek védelme érdekében megfelelő intézkedések megtételére került sor.

h) *A személyes adatokkal összefüggő jogok érvényesítése az érintett halálát követően*

Az érintett halálát követő öt éven belül a jelen Szabályzat III. 9. a-d) pontjában, illetve – Rendelet hatálya alá tartozó adatkezelési műveletek esetén – ezen túl a jelen Szabályzat III.9. f) pontjában meghatározott, az elhaltat életében megillető jogokat az érintett által arra ügyintézési rendelkezéssel, illetve közokiratban vagy teljes bizonyító erejű magánokiratban foglalt, az adatkezelőnél tett nyilatkozattal – ha az érintett egy adatkezelőnél több nyilatkozatot tett, a későbbi időpontban tett nyilatkozattal – meghatalmazott személy jogosult érvényesíteni.

Ha az érintett nem tett az előző bekezdésnek megfelelő jognyilatkozatot, a Ptk. szerinti közeli hozzátartozója annak hiányában is jogosult a III. 9. b) pontjában, a Rendelet hatálya alá tartozó adatkezelési műveletek esetén ezen túl a jelen Szabályzat III. 9. f) pontjában, valamint – ha az adatkezelés már az érintett életében is jogellenes volt vagy az adatkezelés célja az érintett halálával megszűnt – a jelen Szabályzat III. 9. c-d) pontjában meghatározott, az elhaltat életében megillető jogokat érvényesíteni az érintett halálát követő öt éven belül. Az érintett jogainak e bekezdés szerinti érvényesítésére az a közeli hozzátartozó jogosult, aki ezen jogosultságát elsőként gyakorolja.

Az érintett jogait az előzőek alapján érvényesítő személyt e jogok érvényesítése – így különösen az adatkezelővel szembeni, valamint a Hatóság, illetve bíróság előtti eljárás – során az Infotv. által az érintett részére megállapított jogok illetik meg és kötelezettségek terhelik.
Az érintett jogait az első két bekezdés alapján érvényesítő személy az érintett halálának tényét és idejét halotti anyakönyvi kivonattal vagy bírósági határozattal, valamint saját személyazonosságát – és a második bekezdés szerinti esetben közeli hozzátartozói minőségét – közokirattal igazolja.

Az adatkezelő kérelemre tájékoztatja az érintett Ptk. szerinti közeli hozzátartozóját az első két bekezdés alapján megtett intézkedésekről, kivéve, ha azt az érintett az első bekezdésben meghatározott nyilatkozatában megtiltotta.

10. Adatközlések

Személyes adat harmadik személlyel adattovábbítás vagy nyilvánosságra hozatal formájában közölhető.

a) *Személyes adat nyilvánosságra hozatala*

Törvényes közérdekből — az adatok körének kifejezett megjelölésével — elrendelhető a személyes adat nyilvánosságra hozatala.
Az adatok körét az Infotv.-nek közérdekű és közérdekből nyilvános adatokra vonatkozó rendelkezései, a Közzétételi tv., valamint a Közzétételi Szabályzat tartalmazzák. Minden egyéb esetben a nyilvánosságra hozatalhoz az érintett hozzájárulása szükséges. Kétség esetén azt kell vélelmezni, hogy az érintett a hozzájárulását nem adta meg. Az érintett hozzájárulását megadottnak kell tekinteni az érintett közszereplése során az általa közölt vagy nyilvánosságra hozatal céljából általa átadott adatok tekintetében.

b) *Az Európai Unión belüli adattovábbítások (beleértve a belföldre irányuló adattovábbításokat)*

A Társaságon kívüli szervtől vagy magánszemélytől érkező, személyes adat közlésére irányuló megkeresés csak akkor teljesíthető, ha annak jogalapja a III. fejezet 2. pontjában foglaltak szerint fennáll. Az érintett előzetesen is adhat ilyen tartalmú felhatalmazást, amely szólhat meghatározott időtartamra és a megkereséssel élő szervek meghatározott körére.

Az érintett nyilatkozattételétől függetlenül teljesíteni kell a polgári és büntető ügyekben eljáró hatóságoktól — rendőrség, bíróság, ügyészség, NAV, stb. — érkező megkereséseket. Az

adatszolgáltatás csak az adatkezelést végző szervezeti egység munkáltatói jogkör gyakorlója jóváhagyásával teljesíthető.

A nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény 42. §-a szerint az az adatkezelő szerv, amely a nemzetbiztonsági szolgálatok részére az általa kezelt nyilvántartásokból adatszolgáltatást teljesített, adatbetekintést biztosított, illetőleg nyilvántartásában a nemzetbiztonsági szolgálatok megkeresésére jelzést helyezett el, mindezek tényéről, tartalmáról, valamint a megtett intézkedésekről az érintettet, illetőleg más személyt vagy szervezetet nem tájékoztathat.

A megkeresés alapján teljesített **adatszolgáltatással kapcsolatos tényeket, körülményeket jegyzőkönyv (2. számú melléklet)** felvételével dokumentálni kell (kivételt képeznek a hatósági – a Társaság munkavállalóinak munkaviszonyával kapcsolatos – megkeresések, pl. NAV-tól, bíróságtól, nemzetbiztonsági szolgálatoktól érkező megkeresések).

A megkeresésről szóló jegyzőkönyv első példányának megőrzéséről az adatkezelésért felelős szervezeti egység vezetőjének kell gondoskodnia, azt 10 évig kell megőrizni.

c) *Harmadik (Európai Unión kívüli) országba vagy nemzetközi szervezet részére történő adattovábbítások*

Olyan személyes adatok továbbítására – ideértve a személyes adatok harmadik országból vagy nemzetközi szervezettől egy további harmadik országba vagy további nemzetközi szervezet részére történő újbóli továbbítását is –, amelyeket harmadik országba vagy nemzetközi szervezet részére történő továbbításukat követően adatkezelésnek vetnek alá vagy szándékoznak alávetni, csak abban az esetben kerülhet sor, a Rendelet egyéb rendelkezéseinek betartása mellett, ha Társaságunk teljesíti az e pontban rögzített feltételeket. Jelen pont valamennyi rendelkezését alkalmazni kell annak biztosítása érdekében, hogy a természetes személyek számára a Rendeletben garantált védelem szintje ne sérüljön.

A személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására akkor kerülhet sor, ha az Európai Bizottság megállapította, hogy a harmadik ország, a harmadik ország valamely területe, vagy egy vagy több meghatározott ágazata, vagy a szóban forgó nemzetközi szervezet megfelelő védelmi szintet biztosít. Az ilyen adattovábbításhoz nem szükséges külön engedély.

A fenti határozat hiányában Társaságunk csak abban az esetben továbbíthat személyes adatokat harmadik országba vagy nemzetközi szervezet részére, ha megfelelő garanciákat nyújtott, és csak azzal a feltétellel, hogy az érintettek számára érvényesíthető jogok és hatékony jogorvoslati lehetőségek állnak rendelkezésre.

A megfelelő garanciákat az alábbiak jelenthetik:

a) közhatalmi vagy egyéb, közfeladatot ellátó szervek közötti, jogilag kötelező erejű, kikényszeríthető jogi eszköz;
b) a Rendelet 47. cikke szerinti kötelező erejű vállalati szabályok;

c) az Európai Bizottság által a Rendelet 93. cikk (2) bekezdésében említett vizsgálóbizottsági eljárással összhangban elfogadott általános adatvédelmi kikötések;
d) a felügyeleti hatóság által elfogadott és az Európai Bizottság által a Rendelet 93. cikk (2) bekezdésében említett vizsgálóbizottsági eljárásnak megfelelően jóváhagyott általános adatvédelmi kikötések;
e) a Rendelet 40. cikke szerinti, jóváhagyott magatartási kódex a harmadik országbeli adatkezelő vagy adatfeldolgozó arra vonatkozó, kötelező erejű és kikényszeríthető kötelezettségvállalásával együtt, hogy alkalmazza a megfelelő – ideértve az érintettek jogaira vonatkozó – garanciákat; vagy
f) a Rendelet 42. cikke szerinti, jóváhagyott tanúsítási mechanizmus a harmadik országbeli adatkezelő vagy adatfeldolgozó arra vonatkozó, kötelező erejű és kikényszeríthető kötelezettségvállalásával együtt, hogy alkalmazza a megfelelő garanciákat, ideértve az érintettek jogait illetően is.

A NAIH engedélyével a fent említett megfelelő garanciákként különösen az alábbiak is szolgálhatnak:

a) Társaságunk és a harmadik országbeli vagy a nemzetközi szervezeten belüli adatkezelő, adatfeldolgozó vagy a személyes adatok címzettje között létrejött szerződéses rendelkezések; vagy
b) közhatalmi vagy egyéb, közfeladatot ellátó szervek között létrejött, közigazgatási megállapodásba beillesztendő rendelkezések, köztük az érintettek érvényesíthető és tényleges jogaira vonatkozó rendelkezések.

Különös helyzetekben biztosított eltérések:

Az előzőek szerinti megfelelőségi határozat, illetve a fenti megfelelő garanciák hiányában – beleértve a kötelező erejű társasági szabályokat is –, a személyes adatok harmadik ország vagy nemzetközi szervezet részére történő továbbítására vagy többszöri továbbítására csak az alábbi feltételek legalább egyikének teljesülése esetén kerülhet sor:

a) az érintett kifejezetten hozzájárulását adta a tervezett továbbításhoz azt követően, hogy tájékoztatták az adattovábbításból eredő – a megfelelőségi határozat és a megfelelő garanciák hiányából fakadó – esetleges kockázatokról;

b) az adattovábbítás az érintett és Társaságunk közötti szerződés teljesítéséhez, vagy az érintett kérésére hozott, szerződést megelőző intézkedések végrehajtásához szükséges;

c) az adattovábbítás Társaságunk és valamely más természetes vagy jogi személy közötti, az érintett érdekét szolgáló szerződés megkötéséhez vagy teljesítéséhez szükséges;

d) az adattovábbítás fontos közérdekből szükséges;

e) az adattovábbítás jogi igények előterjesztése, érvényesítése és védelme miatt szükséges;

f) az adattovábbítás az érintett vagy valamely más személy létfontosságú érdekeinek védelme miatt szükséges, és az érintett fizikailag vagy jogilag képtelen a hozzájárulás megadására;

g) a továbbított adatok olyan nyilvántartásból származnak, amely az uniós vagy a tagállami jog értelmében a nyilvánosság tájékoztatását szolgálja, és amely vagy általában a nyilvánosság, vagy az ezzel kapcsolatos jogos érdekét igazoló bármely személy számára betekintés céljából hozzáférhető, de csak ha az uniós vagy tagállami jog által a betekintésre megállapított feltételek az adott különleges esetben teljesülnek.

Ha az adattovábbítás nem alapulhat megfelelőségi garanciákon, vagy megfelelőségi határozaton, beleértve a kötelező erejű vállalati szabályok rendelkezéseit is, és a fentiekben említett egyedi helyzetekre vonatkozó eltérések egyike sem alkalmazandó, harmadik országok és nemzetközi szervezetek részére történő adattovábbítás csak akkor történhet, ha az adattovábbítás nem ismétlődő, csak korlátozott számú érintettre vonatkozik, és Társaságunk olyan kényszerítő erejű jogos érdekében szükséges, amely érdekhez képest nem élveznek elsőbbséget az érintett érdekei, jogai és szabadságai, illetve Társaságunk az adattovábbítás minden körülményét megvizsgálta, és e vizsgálat alapján megfelelő garanciákat nyújtott a személyes adatok védelme tekintetében. Társaságunknak tájékoztatnia kell a NAIH-ot az adattovábbításról.

Társaságunk a III. fejezet 7.1 – 7.2. pontjában említett információk nyújtásán kívül az érintettet tájékoztatja az adattovábbításról, valamint Társaságunk kényszerítő erejű jogos érdekéről.

A fenti, különös helyzetekben biztosított eltérések alcím alatt szereplő g) pont szerinti adattovábbítás nem érintheti a nyilvántartásban szereplő személyes adatok vagy személyes adatok kategóriáinak összességét. Ha a nyilvántartásba kizárólag olyan személyek tekinthetnek be, akiknek ehhez jogos érdeke fűződik, az adattovábbításra kizárólag e személyek kérelmére kerülhet sor, illetve abban az esetben, ha ők a címzettek.

A fenti, különös helyzetekben biztosított eltérések alcím alatt szereplő a), b) és c) pontok, valamint második bekezdés nem alkalmazandó a közhatalmi szervek által közhatalmi jogosítványaik gyakorlása során végzett tevékenységekre.
A különös helyzetekben biztosított eltérések alcím alatt szereplő d) pontban említett közérdeket akkor kell figyelembe venni, ha azt az uniós jog vagy Társaságunkra vonatkozó tagállami jog elismeri.

Megfelelőségi határozat hiányában az uniós jog vagy a tagállami jog fontos közérdekből kifejezetten korlátozhatja bizonyos kategóriákba tartozó személyes adatok valamely harmadik országba vagy nemzetközi szervezethez történő továbbítását.

Az **adatszolgáltatással kapcsolatos tényeket, körülményeket jegyzőkönyv (3. számú melléklet)** felvételével dokumentálni kell.

A megkeresésről szóló jegyzőkönyv első példányának megőrzéséről az adatkezelésért felelős szervezeti egység vezetőjének kell gondoskodnia. A jegyzőkönyv második példányát az adatvédelmi tisztviselőhöz kell továbbítani. A jegyzőkönyvet 10 évig kell megőrizni.

11. Közös adatkezelés

Ha az adatkezelés céljait és eszközeit Társaságunk és további egy vagy több adatkezelő közösen határozza meg, közös adatkezelőknek minősülnek. A közös adatkezelők átlátható módon, a közöttük létrejött megállapodásban kötelesek meghatározni a Rendelet és jelen Szabályzat szerinti kötelezettségek teljesítéséért fennálló, különösen az érintett jogainak gyakorlásával és a jelen Szabályzat III. fejezet 7.1 és 7.2 pontjában említett információk rendelkezésre bocsátásával kapcsolatos feladataikkal összefüggő felelősségük megoszlását, kivéve azt az esetet és annyiban, ha és amennyiben Társaságunkra vonatkozó felelősség megoszlását a rájuk alkalmazandó uniós vagy tagállami jog határozza meg. A megállapodásban az érintettek számára kapcsolattartót lehet kijelölni.

A fenti bekezdésben említett megállapodásnak megfelelően tükröznie kell a közös adatkezelők érintettekkel szembeni szerepét és a velük való kapcsolatukat. A megállapodás lényegét az érintett rendelkezésére kell bocsátani. Az érintett a fenti bekezdésben említett megállapodás feltételeitől függetlenül mindegyik adatkezelő vonatkozásában és mindegyik adatkezelővel szemben gyakorolhatja a Rendelet szerinti jogait.

12. Az adatfeldolgozó igénybevételének szabályai

Társaságunk az adatok feldolgozásával kapcsolatos műveletek elvégzésére adatfeldolgozót vehet igénybe.

Jelen Szabályzat I. fejezet 4. pontja szerint adatfeldolgozás: az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől, feltéve hogy a technikai feladatot az adatokon végzik; adatfeldolgozó: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely Társaságunk nevében személyes adatokat kezel.

Az adatfeldolgozónak a személyes adatok feldolgozásával kapcsolatos jogait és kötelezettségeit a Rendelet 28. cikke, valamint az adatkezelésre vonatkozó külön törvények keretei között Társaságunk határozza meg. **Az adatfeldolgozásra vonatkozó megbízási szerződést írásba kell foglalni, és a szerződésnek tartalmaznia kell a Rendelet 28. cikkének (3)-(4) bekezdésében foglalt kritériumokat.**

a) *Társaságunk felelőssége*

- Az adatkezelési műveletekre vonatkozó szabályozások jogszerűségéért Társaságunk felel.
- A Társaság külső adatfeldolgozót is igénybe vehet.
- Adatfeldolgozásra nem adható megbízás olyan vállalkozásnak, amely a feldolgozandó személyes adatokat felhasználó üzleti tevékenységben érdekelt.
- A Társaság által igénybe vett adatfeldolgozó esetében szerződésben meghatározott szigorú szabályok szerint kell eljárni, melyek betartásáról rendszeres ellenőrzéssel kell meggyőződni (az ellenőrzésről a szerződés teljesítésével kapcsolatban felelős szervezeti egység vezetőjének kell gondoskodnia).

b) *Az adatfeldolgozó felelőssége*

- Az adatfeldolgozó tevékenységi körén belül, illetőleg a Társaságunk által meghatározott keretek között felelős a személyes adatok feldolgozásáért, megváltoztatásáért, törléséért, továbbításáért és nyilvánosságra hozataláért.
- Az adatfeldolgozó tevékenységének ellátása során más adatfeldolgozót Társaságunk előzetes írásbeli, eseti vagy általános felhatalmazása szerint vehet igénybe, figyelemmel a Rendelet 28. cikkének (4) bekezdésében foglalt megkötésekre is.
- Az adatfeldolgozó az adatkezelést érintő érdemi döntést nem hozhat, a tudomására jutott személyes adatokat kizárólag Társaságunk rendelkezései szerint dolgozhatja fel, saját céljára adatfeldolgozást nem végezhet, továbbá a személyes adatokat Társaságunk rendelkezései szerint köteles tárolni és megőrizni.

Az adatfeldolgozó és bármely, Társaságunk vagy az adatfeldolgozó irányítása alatt eljáró, a személyes adatokhoz hozzáféréssel rendelkező személy ezeket az adatokat kizárólag Társaságunk szabályozásainak megfelelően kezelheti, kivéve, ha az ettől való eltérésre őt uniós vagy tagállami jog kötelezi.

IV. FEJEZET

A KÖZÉRDEKŰ ADATOK NYILVÁNOSSÁGÁRA VONATKOZÓ ELŐÍRÁSOK

Az Infotv. rendelkezései alapján a Társaság, mint közfeladatot ellátó szerv, a feladatkörébe tartozó ügyekben — így különösen a közösségi közlekedésre vonatkozó közérdekű információkkal — köteles elősegíteni és biztosítani a közvélemény pontos és gyors tájékoztatását. A Társaság rendszeresen közzé- vagy más módon hozzáférhetővé teszi a tevékenységével kapcsolatos legfontosabb adatokat a Közzétételi Szabályzatban foglaltaknak megfelelően.

A Társaságnak lehetővé kell tennie, hogy a kezelésében lévő közérdekű adatot bárki megismerhesse, illetve ha a közérdekű adatok nyilvánosságához való jogot — az adatfajták meghatározásával

- honvédelmi,
- nemzetbiztonsági,
- bűnüldözési vagy bűnmegelőzési,
- környezet-, vagy természetvédelmi érdekből,
- központi pénzügyi vagy devizapolitikai érdekből,
- külügyi kapcsolatokra, nemzetközi szervezetekkel való kapcsolatokra,
- bírósági vagy közigazgatási hatósági eljárásra tekintettel,
- a szellemi tulajdonhoz fűződő jogra tekintettel

törvény korlátozza.

A Társaság hatáskörében eljáró személynek a feladatkörével összefüggő személyes adata a közérdekű adat megismerését nem korlátozza.

Ha törvény másként nem rendelkezik, a Társaság feladat- és hatáskörébe tartozó döntés meghozatalára irányuló eljárás során készített vagy rögzített, a döntés megalapozását szolgáló

adat a keletkezésétől számított tíz évig nem nyilvános. Kérelemre az adatok megismerését az ügyvezető e határidőn belül is engedélyezheti.
A közérdekű adatok megismerésével és nyilvánosságával összefüggésben az üzleti titok megismerésére a Ptk.-ban foglaltak jelen Szabályzatban foglalt eltérésekkel az irányadók.

A közérdekű adat megismerése

A közérdekű adatok megismerésére irányuló — szóban, írásban vagy elektronikus úton érkező — kérelemnek az adatkezelésért felelős szervezeti egység vezetője a kérelem tudomására jutását követő legrövidebb idő alatt, legfeljebb azonban 15 napon belül, közérthető formában tesz eleget.

Ha az adatigénylés jelentős terjedelmű, illetve nagyszámú adatra vonatkozik, a teljesítésre meghatározott 15 napos határidő egy alkalommal 15 nappal meghosszabbítható. Erről az igénylőt az igény kézhezvételét követő 15 napon belül tájékoztatni kell.

Amennyiben az adatigényléshez kapcsolódóan a 2. pontban foglaltak szerint költségtérítés megállapítására kerül sor, az adatigénylés teljesítésének határideje tekintetében a 2. pont rendelkezései is irányadók.

Az adatokat tartalmazó dokumentumról vagy dokumentumrészről annak tárolási módjától függetlenül a kérelmező másolatot kérhet, illetve összetett adatkérés esetén (amely az igényelt adatok felkutatásával, összesítésével és rendszerezésével jár) külön dokumentumot kell összeállítani.

Társaságunk a másolat készítéséért a külső fél részére végzett szolgáltatási tevékenységek folyamatainak szabályozásáról szóló, mindenkor hatályos utasításban (a továbbiakban: Utasítás)) meghatározott esetekben és összegek alapul vételével költségtérítést állapíthat meg, amelynek összegéről az adatkezelést végző szervezeti egység érintett szakterületének az igénylőt az igény teljesítését megelőzően tájékoztatni kell.

Az igénylő a tájékoztatás kézhezvételét követő 30 napon belül nyilatkozik arról, hogy az igénylését fenntartja-e. A tájékoztatás megtételétől az igénylő nyilatkozatának Társaságunkhoz való beérkezéséig terjedő időtartam az adatigénylés teljesítésére rendelkezésre álló határidőbe nem számít bele. Ha az igénylő az igényét fenntartja, a költségtérítést a nyilatkozat keltétől (ennek hiányában a postára adásától) számított 15 napon belül köteles Társaságunk részére – az Utasításban meghatározott módon – megfizetni. Erre az igénylőt az adatkezelést végző szervezeti egység érintett szakterülete a fenti tájékoztatásban szintén köteles felhívni.

Ha az adatigénylés teljesítése Társaságunk alaptevékenységének ellátásához szükséges munkaerőforrás aránytalan mértékű igénybevételével jár, vagy az a dokumentum vagy dokumentumrész, amelyről az igénylő másolatot igényelt, jelentős terjedelmű, illetve a költségtérítés mértéke meghaladja a közérdekű adat iránti igény teljesítéséért megállapítható költségtérítés mértékéről szóló 301/2016. (IX. 30.) Kormányrendeletben meghatározott összeget (jelenleg 5.000.- forintot), az adatigénylést a költségtérítésnek az igénylő általi megfizetését követő 15 napon belül kell teljesíteni.

Arról, hogy az adatigénylés teljesítése Társaságunk alaptevékenységének ellátásához szükséges humánerőforrás aránytalan mértékű igénybevételével jár, illetve a másolatként igényelt dokumentum vagy dokumentumrész jelentős terjedelmű, továbbá a költségtérítés mértékéről, a fizetés előzőekben meghatározott feltételeiről, határidejéről, valamint az adatigénylés teljesítésének a másolatkészítést nem igénylő lehetőségeiről az igénylőt az igény beérkezését követő 15 napon belül tájékoztatni kell.

Ha a közérdekű adatot tartalmazó dokumentum az igénylő által meg nem ismerhető adatot is tartalmaz, a másolaton a meg nem ismerhető adatot felismerhetetlenné kell tenni.

Az adatigénylésnek közérthető formában és – amennyiben ezt a Társaság aránytalan nehézség nélkül teljesíteni képes – az igénylő által kívánt technikai eszközzel, illetve módon kell eleget tenni.

Ha a kért adatot a Társaság korábban már elektronikus formában nyilvánosságra hozta, az igény teljesíthető az adatot tartalmazó nyilvános forrás megjelölésével is.

Az adatigénylést nem lehet elutasítani arra való hivatkozással, hogy annak közérthető formában nem lehet eleget tenni.

A közérdekű adat megismerésére vonatkozó kérelem megtagadása

A kérelem megtagadásáról — annak indokaival együtt — 15 napon belül írásban értesíteni kell a kérelmezőt, valamint az adatvédelmi tisztviselőt.
Az adatvédelmi tisztviselő évente, minden év január 31. napjáig értesíti a NAIH-ot az elutasított kérelmekről, valamint az elutasítások indokairól.

Ha a közérdekű adatokra vonatkozó kérését nem teljesítik, a kérelmező a bírósághoz fordulhat. A megtagadás jogszerűségét és megalapozottságát a Társaság köteles bizonyítani. A kérelem megtagadása esetén — a bírósági eljárást megelőzendő — az adatkezelést végző szervezeti egység érintett szakterülete vezetőjének az adatvédelmi tisztviselő tájékoztatásával egyidejűleg a Jogi és Humánpolitikai Igazgatóság állásfoglalását kell kérnie (ettől függetlenül a kérelmező — és vele egyidejűleg az adatvédelmi tisztviselő — írásos értesítése 8 napon belül kell, hogy megtörténjen, így a megkereséseket ennek figyelembevételével kell megtenni).

A bíróság előtti eljárásban a Társaság képviseletét a Jogi és Humánpolitikai Igazgatóság látja el.

A közérdekből nyilvános adatok megismerésére a közérdekű adatok megismerésére vonatkozó rendelkezéseket kell alkalmazni.

V. FEJEZET

AZ ADATBIZTONSÁG ÉS TECHNIKAI HÁTTERÉNEK EGYES KÉRDÉSEI, IRATMINŐSÍTÉSI ALAPELVEK

1. Az adatkezelés biztonsága

Társaságunk a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket köteles végrehajtani annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja, ideértve, többek között, adott esetben:

a) a személyes adatok álnevesítését és titkosítását;

b) a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítását, sértetlenségét rendelkezésre állását és ellenálló képességét;

c) fizikai vagy műszaki incidens esetén az arra való képességet, hogy a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását kellő időben vissza lehet állítani;

d) az adatkezelés biztonságának garantálására hozott technikai és szervezési intézkedések hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárást.

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

Társaságunk köteles intézkedéseket hozni annak biztosítására, hogy az irányítása alatt eljáró, a személyes adatokhoz hozzáféréssel rendelkező természetes személyek kizárólag Társaságunk szabályozásainak megfelelően kezelhessék az említett adatokat, kivéve, ha az ettől való eltérésre uniós vagy tagállami jog kötelezi őket.

Külön kiemelendő ebben a körben az álnevesítés intézménye, mely csökkentheti az érintettek számára a kockázatokat, valamint segíthet Társaságunknak és az adatfeldolgozóknak abban, hogy az adatvédelmi kötelezettségeiknek megfeleljenek.

Jelen fejezetben felsorolt intézkedések a törvényi szabályozások leképezései, **a szakmai és technikai szabályokat, eljárásokat az Informatikai Biztonsági Szabályzat tartalmazza részletesen.**

2. Az adatvédelmi incidensek kezelése

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.

Az adatvédelmi incidens kivizsgálására vonatkozó szabályok

A Társaság által kezelt személyes adatokat érintő ilyen esemény kapcsán az adatvédelmi tisztviselőt az eseményről a lehető legrövidebb időn belül tájékoztatni kell, továbbá az esemény kapcsán kezdeményezett vizsgálatba (ellenőrzésbe) be kell vonni.

Amennyiben az adatvédelmi incidens érinti az Társaság informatikai rendszerét is, akkor a tájékoztatást az informatikai főosztályvezetőnek is meg kell küldeni és a vizsgálatba szintén be kell vonni.

A vizsgálatnak ki kell térnie arra, hogy az adatvédelmi incidens magas kockázattal jár-e az érintettek jogaira és kötelezettségeire, milyen jellegű kockázatról van szó és szükséges-e az érintettek tájékoztatása az incidensről. Amennyiben nem szükséges az érintettek tájékoztatása, a vizsgálatnak ki kell térnie ennek indokaira is.

A vizsgálat eredményeként az adatvédelmi tisztviselő javaslatot tesz az adatvédelmi incidenssel érintett adatkezelést végző szervezeti egység vezetőjének az incidens kezeléshez szükséges intézkedések megtételére.

A javaslat alapján a megvalósítandó további intézkedésekről az adatkezelésért felelős szervezeti egység vezetője – informatikai rendszerben bekövetkezett adatvédelmi incidens esetében az informatikai főosztályvezető egyetértésével – dönt.

A vizsgálatot indokolatlan késedelem nélkül, ha lehetséges, legkésőbb az incidensről történő tudomásszerzéstől számított 72 órán belül le kell zárni, oly módon, hogy a Társaság az adatvédelmi incidens bejelentésére vonatkozó alábbi kötelezettségnek is eleget tudjon tenni.

Az adatvédelmi incidens bejelentése

Adatvédelmi incidenst – az adatvédelmi tisztviselő közreműködésével – az adatkezelést végző szervezeti egység vezetője köteles indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, bejelenteni a NAIH erre szolgáló felületén (http://www.naih.hu/adatvedelmi-incidensbejelent--rendszer.html), kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Ha a bejelentés nem történik meg 72 órán belül, mellékelni kell hozzá a késedelem igazolására szolgáló indokokat is.

A fent említett bejelentésben legalább:

a) ismertetni kell az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát;
b) közölni kell az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;
c) ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket;
d) ismertetni kell a Társaságunk által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

Ha és amennyiben nem lehetséges az információkat egyidejűleg közölni, azok további indokolatlan késedelem nélkül később részletekben is közölhetők.

Az adatkezelést végző szervezeti egység vezetője köteles biztosítani az adatvédelmi incidensek nyilvántartását, feltüntetve az adatvédelmi incidenshez kapcsolódó tényeket, annak hatásait és az orvoslására tett intézkedéseket.

Az érintett tájékoztatása az adatvédelmi incidensről

Az adatkezelést végző szervezeti egység vezetője köteles gondoskodni arról, hogy amennyiben az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, Társaságunk indokolatlan késedelem nélkül tájékoztassa az érintettet az adatvédelmi incidensről.

Az érintett részére adott tájékoztatásban világosan és közérthetően ismertetni kell az adatvédelmi incidens jellegét, és közölni kell legalább a fenti b), c) és d) alpontokban említett információkat és intézkedéseket.

Az érintettet nem kell a fentiek szerint tájékoztatni, ha a következő feltételek bármelyike teljesül:

a) Társaságunk megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre, és ezeket az intézkedéseket az adatvédelmi incidens által érintett adatok tekintetében alkalmazták, különösen azokat az intézkedéseket – mint például a titkosítás alkalmazása –, amelyek a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik az adatokat;
b) Társaságunk az adatvédelmi incidenst követően olyan további intézkedéseket tett, amelyek biztosítják, hogy az érintett jogaira és szabadságaira jelentett, a fent említett magas kockázat a továbbiakban valószínűsíthetően nem valósul meg;
c) a tájékoztatás aránytalan erőfeszítést tenne szükségessé. Ilyen esetekben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, vagy olyan hasonló intézkedést kell hozni, amely biztosítja az érintettek hasonlóan hatékony tájékoztatását.

Ha Társaságunk még nem értesítette az érintettet az adatvédelmi incidensről, a NAIH, miután mérlegelte, hogy az adatvédelmi incidens valószínűsíthetően magas kockázattal jár-e, elrendelheti az érintett tájékoztatását, vagy megállapíthatja a mentesülés fent említett feltételei közül valamelyik teljesülését.

3. **Az infrastruktúrához kapcsolódó védelmi intézkedések**

Irattáraknál, zárt helyiségbe (pl. gépterem) történő informatikai eszközök telepítésénél, biztosítani kell a tűzvédelmet, a fizikai biztonságot, a ki- és belépés ellenőrzött rendjét, az illetéktelen bejutást gátló eszközök üzembiztos működését, valamint az informatikai eszközök karbantartása esetén garantálni kell a gyártó cégek előírásainak betartását.
A biztonságtechnikai eszközök működését rendszeresen ellenőrizni kell, és gondoskodni kell a biztonságtechnikai berendezések rendszeres karbantartásáról.

a) *Szervertermek üzemeltetési rendje, biztonsági előírásai*

A részletes rendelkezéseket az Informatikai Biztonsági Szabályzat tartalmazza.

b) *Adatok, adatcsoportok besorolása információbiztonsági szempontból*

A kezelt adatokat, adatcsoportokat információbiztonsági szempontból három szempont szerint, öt fokozatú skálán kell besorolni. A besorolást szerepeltetni kell az információleltárban, vagy más néven adatvagyon leltárban. Az információs leltárban rögzített vagyonelemeken elvégzett kockázatértékelés eredményeként meghatározott kockázati szintek alapján az adatokat, adatcsoportokat öt biztonsági kategóriába soroljuk. Az egyes informatikai rendszerekre vonatkozó védelmi intézkedéseket a bennük tárolt adatok, adatcsoportok besorolása alapján kell meghatározni.

Az adatokat, adatcsoportokat a következő szempontok szerint kell besorolni:

- az információ bizalmassága
- az információ sértetlensége, illetve
- az információ rendelkezésre állása

szempontjából.

Az információ bizalmassága szerinti osztályozás

A besorolás megegyezik a II. fejezet 4. pontjában foglaltakkal.

Az információ sértetlensége szerinti osztályozás

A sértetlenség alapján történő osztályozás során meg kell vizsgálni, hogy az adatok pontosságának, teljességének vagy sértetlenségének elvesztése milyen következményekkel járhat.

A hatások szempontjából: szempontjából pénzügyi, jogi, hírnévvel kapcsolatos, reputációs és működési károkat különböztetünk meg.

Sértetlenség szempontjából megkülönböztetünk általánosan, fokozottan és kiemelten védendő adatokat, adatcsoportokat.

- Általánosan védettek az adatok, adatcsoportok, ha a sértetlenségi besorolásuk 1-es. Ide tartoznak a jellemzően belső használatra vagy tájékoztatásra szánt adatok, amelyek adattartalmának sérülése és a sérült adattartalom felhasználása kapcsán anyagi kár nem keletkezhet. A normál munkavégzésben a sérülés okán felmerült probléma torlódást nem okoz. Jogi következményre és hírnévvesztésre nem kell számítani.
- Fokozottan védettek az adatok, adatcsoportok, ha a sértetlenségi besorolásuk 2-es vagy 3-as. Ebben az esetben az adattartalom sérülése és a sérült adatok felhasználása kapcsán anyagi kár nem vagy csak csekély mértékben keletkezik, de érdemben befolyásolhatja a szervezet működését, a normál munkavégzésben torlódás jelentkezhet. A munkavégzés nehézkesebbé válik, de a sérülés korrigálása a napi munkavégzés során megoldható. Jogi következményre lehet számítani, ügyfél elégedetlenség és hírnévveszteség is jelentkezhet.
- Kiemelten védettek az adatok, adatcsoportok, ha a sértetlenségi besorolásuk 4-es vagy 5-ös. Olyan adatok tartoznak ide, melyek tartalmának sérülése és a sérült adattartalom felhasználása kapcsán akár jelentősebb anyagi kár is keletkezhet. A munkavégzésben jelentős fennakadás csak túlmunkával kompenzálható, nagyon súlyos esetben a Társaság egyes funkcióinak ellátása korlátozott időre megbénulhat. Akár tömeges peres eljárások is indulhatnak a Társaság ellen, mely következtében hosszabb távú hírnévveszteséggel kell számolni.

Az információ rendelkezésre állása alapján történő osztályozás

A rendelkezésre állás szempontjából üzletileg nem kritikus és kritikus adatokat, adatcsoportokat különböztetünk meg.

- Üzletileg nem kritikusak az adatok, adatcsoportok, ha a rendelkezésre állás szempontjából a besorolásuk 1-es, 2-es vagy 3-as. Ide tartoznak azok az adatok, amelyek rendelkezésre NEM állása kapcsán az érintett folyamatokban jelentősebb pénzügyi veszteség nem realizálódik, több területre kiterjedő túlmunkát a Társaság munkavállalóinak nem okoz és hiányuk nem generál komolyabb külső elégedetlenséget, hírnévveszteséget illetve jogi fenyegetettséget.
- Üzletileg kritikusak az adatok, adatcsoportok, ha a rendelkezésre állás szempontjából a besorolásuk 4-es vagy 5-ös. Ide tartoznak azok az adatok, amelyek rendelkezésre NEM állása kapcsán jelentős pénzügyi veszteség realizálódhat és/vagy komolyabb túlmunkát generálhatnak a napi munkavégzésen túl, valamint a kapcsolódó folyamatok végrehajtását akadályozhatják. Hírnévvesztés, külső és belső elégedetlenség, illetve jogi fenyegetés vagy akár per egyaránt előfordulhat.

A rendelkezésre állás a következő időértékeken értelmezhető:

- 1 óra,
- 4 óra,
- 1 nap,
- 5 nap.

A besorolással kapcsolatos további részletes rendelkezéseket az Informatikai Biztonsági Szabályzat tartalmazza.

4. **A hardverekhez kapcsolódó védelmi intézkedések**

A hardverekhez kapcsolódó védelmi intézkedések részletes rendjét az Informatikai Biztonsági Szabályzat tartalmazza.

Az Informatikai Főosztálynak — a Társaság részére szerződés alapján informatikai szolgáltatásokat nyújtó IT-szolgáltató bevonásával — gondoskodnia kell azon háttértárakon elhelyezett információk visszaállíthatatlan (végleges) törlésére, melyeket az IT-szolgáltató bármilyen okból kifolyólag (pl. szervizelés, gépcsere) elszállít. Az Informatikai Főosztálynak gondoskodnia kell a társasági mobil eszközökön elhelyezett információk visszaállíthatatlan (végleges) törléséről is az eszközök leadása esetén. Ennek részleteit az Informatikai Biztonsági Szabályzat írja elő.

5. **A szoftverekhez kapcsolódó védelmi intézkedések**

A szoftverekhez kapcsolódó védelmi intézkedések részletes rendjét az Informatikai Biztonsági Szabályzat tartalmazza.

Külső szakértők számára — az IT-szolgáltató szakembereinek kivételével — a Társaság „éles” adatait tartalmazó adatbázisokkal való műveletvégzés nem engedélyezett, a munkavégzés során kizárólag az „éles” rendszertől elkülönített, anonimizált adatok használhatók fel. A külső szakértővel ilyen esetben titoktartási nyilatkozatot kell aláíratni szerződéskötéskor.

6. **Katasztrófahelyzetek kezelése**

Az adatbiztonság témakörét érintő katasztrófahelyzetek kezelésének részleteit az Informatikai Biztonsági Szabályzat írja elő.

7. **Az adathordozókhoz kapcsolódó védelmi intézkedések**

A különböző adathordozók (pl. mágneses, optikai adathordozók) használatának rendjét, az adathordozók tartalmáról történő másolatok készítésének és tárolásának rendjét, az adathordozók raktározási, nyilvántartási, hozzáférési és selejtezési rendjét, valamint azok archiválási rendjét az Informatikai Biztonsági Szabályzat tartalmazza.

8. **Az információ kezelésével kapcsolatos intézkedések**

Minden, nem nyilvános bizalmassági besorolású adatot, adatcsoportot tartalmazó információ-feldolgozó rendszerrel történő munkavégzés során az alábbiakat kell betartani:

- Azokra a munkafolyamatokra, ahol a nem nyilvános bizalmassági besorolású adatot, adatcsoportot tartalmazó adathordozók mozgatása, átadása nem kerülhető el, pontosan meg kell határozni a jogosult átvevőinek körét, az átadás-átvétel szabályait. Ez vonatkozik a feldolgozási folyamatok során nyomtatott listákra is.
- A nem nyilvános bizalmassági besorolású adatot, adatcsoportot tartalmazó elektronikus dokumentumokba (pl. Word, Excel dokumentum) külső dokumentumot csatolással

beilleszteni tilos, mert a csatolt állomány esetleges törlésével a bizalmas dokumentum információtartalma sérülhet.

- A nem nyilvános bizalmassági besorolású adatot, adatcsoportot, információkat tartalmazó dokumentumokat, vagy azokból kiemelt részeket nem bizalmas besorolású elektronikus dokumentumokba (pl. Word, Excel dokumentum) beilleszteni, vagy azokban hivatkozást elhelyezni tilos, mert ezúton bizalmas információ kerülhet illetéktelenekhez.
- A nem nyilvános bizalmassági besorolású adatot, adatcsoportot tartalmazó dokumentum nyomtatását követően a nyomtatóból azt azonnal ki kell venni. A hálózati nyomtatóból a nyomatot csak kártyás azonosítás után lehet kivenni.
- Mindazok részére, akik a különféle engedélyeket, feljogosító igazolásokat ellenőrizhetik (pl. biztonsági szolgálat), erre a célra aláírás mintákat kell kiadni. A mintának arra is ki kell terjednie, hogy az engedélyezőnek milyen típusú engedélyt szabad kiadnia. Az engedélyeket formalizálni kell.
- A munkafolyamatok megszakítása idejére (pl. ebédszünet) a nem nyilvános bizalmassági besorolású adatot, adatcsoportot tartalmazó információkat tartalmazó adathordozókat, kinyomtatott dokumentumokat, a rosszindulatú hozzáféréstől és a sérülésektől védetten kell tárolni, zárt iratszekrényben (a szigorúan bizalmas adathordozókat páncélszekrényben (kazettában) vagy más, ezt lehetővé tevő módon..

9. Személyes adatok törlése az adatkezelés jogalapjának megszűnését követően

Az informatikai rendszerekben kezelt adatok esetében biztosítani kell az adatkezelés jogalapjának megszűnését követően a személyes adatok - ide értve a különleges adatokat is – törlését. Ennek biztosítása érdekében az adatkezelést végző szervezeti egység vezetőjének – az erre vonatkozó szakterületi részletszabályozás kidolgozásával – meg kell határoznia a törlésre előirányzott határidőket, ahol lehetséges, ott összhangban az Iratkezelési Szabályzat 2. számú mellékletében meghatározott megőrzési időkkel. Az informatikai alkalmazások esetében – amennyiben az adott alkalmazás ilyen folyamatot nem tartalmaz – ki kell alakítani azokat a paraméterezhető automatizmusokat, amelyekkel a törlés végrehajtható, vagy a törlendő adat anonimizálásra kerül.

Azon rendszerek esetében, ahol a tudomány és technológia állása és a megvalósítás költségei az adattörlést, vagy az anonimizálást nem teszik lehetővé, de a törlésre jelölt adatokhoz való hozzáférés a továbbiakban manuális munkafolyamattal elkerülhető, az adatgazda feladata a törlésre jelölt adatokhoz való hozzáférés elkerülésére manuális munkafolyamat kialakítása és működtetése.

Az adatok törléséről az elektronikus levelezésben tárolt adatok esetében a postaláda használatára jogosult, a fájlrendszerben tárolt adatok esetében a mappa létrehozását igénylő vezető köteles gondoskodni.

Az informatikai rendszerben kezelt adatok törlésekor – amennyiben az Iratkezelési Szabályzat eltérően nem rendelkezik – gondoskodni kell azok papíron tárolt, nyomtatott változatának megsemmisítéséről is.

10. **Iratminősítési alapelvek**

A Társaságon belüli megjelölések:

- üzleti titok („Üzleti titok” megjelöléssel; lsd. II. fejezet 3. e) pont, minősítésre jogosultak: vezérigazgató-helyettesek, igazgatók, irodavezetők, főosztályvezetők),
- nem nyilvános irat („Nem nyilvános” megjelöléssel), valamint
- nyílt irat (megjelölés nélkül).
- a fenti megjelölés mellett fel kell tüntetni az iraton annak jelen Szabályzat II.4. pontja szerinti bizalmassági kategóriáját is a következő módon: „Az irat társasági bizalmassági kategóriája:…”

„Nem nyilvános” kategória

Minden olyan tény, információ, megoldás vagy adat, amely nem tartozik az „Üzleti titok” kategóriába, de a nyilvános iratoktól megkülönböztetve kezelendő (pl. döntéselőkészítő iratok). A kezelési előírások megsértése esetén munkajogi felelősségre vonás kezdeményezhető.

Minősítésre jogosult: az illetékes szakterületi legfelsőbb vezetői, tehát az ügyvezető, a telephely vezetők.

„Nyílt irat” kategória

Minden olyan tény, információ, megoldás vagy adat, amely nem tartozik sem az „Üzleti titok”, sem pedig a „Nem nyilvános” kategóriába.
Mivel kezelésük nem igényel különleges előírásokat, ezért nincs szükség minősítésre jogosultak meghatározására sem.

A fenti minősítési kategóriákhoz tartozó **konkrét kezelési előírásokat** — végrehajtási rész — az Iratkezelési Szabályzat, az informatikai rendszerek használata során betartandó biztonsági előírásokat pedig az Informatikai Biztonsági Szabályzat tartalmazza részletesen.

11. **Az üzleti titok (II.3.d) pont) és a munkakör betöltésével összefüggésben a munkavállalók tudomására jutott adatok védelme**

Valamennyi szervezeti egység vezetője köteles gondoskodni minden olyan tény, tájékoztatás, egyéb adat és az azokból készült összeállítás (a továbbiakban együtt: információ) tekintetében, amely a Társaság üzleti titkának minősül, valamint a harmadik személyek üzleti titokként rendelkezésre álló információi tekintetében az alábbiakról:

- az üzleti titok ne kerülhessen illetéktelen harmadik személy birtokába vagy nyilvánosságra, ne válhasson ilyen körben hozzáférhetővé;
- harmadik személynek csak jogszerűen, indokolt esetben bocsássanak rendelkezésre vagy tegyenek hozzáférhetővé üzleti titkot, titoktartási nyilatkozat mellett;
- az, akinek az üzleti titkot rendelkezésére bocsátják, hozzáférhetővé teszik, szükség szerint általánosságban vagy esetenként tájékoztatást kapjon arról, hogy az adott információ üzleti titoknak minősül;

- a Társaság által megkötött polgári jogi szerződésekben rögzítve legyenek az üzleti titok védelmére vonatkozó rendelkezések;
- üzleti titok birtokába csak olyan munkavállalók juthassanak, akiknek ez a munkaköre ellátásához feltétlenül szükséges.

Az Mt. 8. § (4) bekezdése értelmében a munkavállaló köteles a munkája során tudomására jutott üzleti titkot megőrizni. Ezen túlmenően sem közölhet illetéktelen személlyel olyan adatot, amely munkaköre betöltésével összefüggésben jutott a tudomására, és amelynek közlése a munkáltatóra vagy más személyre hátrányos következménnyel járhat.

A munkavállalónak az együttműködési kötelezettségéből eredően is fokozott gondossággal kell eljárnia, ennek keretében a tudomására jutott információk közlése, hozzáférhetővé tétele előtt fel kell mérnie azt, hogy melyek azok az információk, amelyek esetében felmerül az Mt. fenti rendelkezéseinek megsértése abban az esetben, ha azok illetéktelen harmadik személyhez vagy nyilvánosságra jutnak, ilyen körben hozzáférhetővé válnak.

A munkavégzés keretében a munkáltatói jogkör gyakorlójának jóváhagyása nélkül üzleti titoknak minősülő információ harmadik személlyel és a nyilvánossággal nem közölhető, ilyen körben nem tehető hozzáférhetővé.

A titoktartás nem terjed ki a közérdekű adatok nyilvánosságára és a közérdekből nyilvános adatra vonatkozó, törvényben meghatározott adatszolgáltatási és tájékoztatási kötelezettségre.

VI. FEJEZET

AZ ADATVÉDELMI TISZTVISELŐ FELADATAI, JOGAI, KÖTELEZETTSÉGEI ÉS FELELŐSSÉGE

1. Az adatvédelmi tisztviselő jogállása

Az adatkezelést végző valamennyi szervezeti egység vezetője köteles biztosítani, hogy az adatvédelmi tisztviselő a személyes adatok védelmével kapcsolatos összes ügybe megfelelő módon és időben bekapcsolódjon.

A Rendelet alapján Társaságunk köteles támogatni az adatvédelmi tisztviselőt feladatai ellátásában azáltal, hogy biztosítja számára azokat az forrásokat, amelyek e feladatok végrehajtásához, a személyes adatokhoz és az adatkezelési műveletekhez való hozzáféréshez, valamint az adatvédelmi tisztviselő szakértői szintű ismereteinek fenntartásához szükségesek.

Társaságunk biztosítja, hogy az adatvédelmi tisztviselő a feladatai ellátásával kapcsolatban utasításokat senkitől ne fogadjon el. Az adatvédelmi tisztviselőt feladatai ellátásával összefüggésben nem bocsátható el és szankcióval nem sújtható. Az adatvédelmi tisztviselő közvetlenül az Társaság legfelső vezetésének tartozik felelősséggel.

Az érintettek a személyes adataik kezeléséhez és jogaik gyakorlásához kapcsolódó valamennyi kérdésben az adatvédelmi tisztviselőhöz fordulhatnak.

Az adatvédelmi tisztviselőt feladatai teljesítésével kapcsolatban uniós vagy tagállami jogban meghatározott titoktartási kötelezettség vagy az adatok bizalmas kezelésére vonatkozó kötelezettség köti.

Az adatvédelmi tisztviselő más feladatokat is elláthat. Társaságunk biztosítja, hogy e feladatokból ne fakadjon összeférhetetlenség.

Az adatvédelmi tisztviselő feladatait az adatkezelési műveletekhez fűződő kockázat megfelelő figyelembevételével, az adatkezelés jellegére, hatókörére, körülményére és céljára is tekintettel végzi.

2. Az adatvédelmi tisztviselő feladatai

- Tájékoztat és szakmai tanácsot ad a Társaság, továbbá az adatkezelést végző alkalmazottak részére a Rendelet, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezések szerinti kötelezettségeikkel kapcsolatban.
- Ellenőrzi a Rendeletnek, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezéseknek, továbbá az Társaság személyes adatok védelmével kapcsolatos belső szabályainak való megfelelést, ideértve a feladatkörök kijelölését, az adatkezelési műveletekben vevő személyzet tudatosság-növelését és képzését, valamint a kapcsolódó auditokat is.

- Kérésre szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, valamint nyomon követi a hatásvizsgálat elvégzését.
- Együttműködik a NAIH-al és az adatkezeléssel összefüggő ügyekben kapcsolattartó pontként szolgál felé, valamint adott esetben bármely egyéb kérdésben konzultációt folytat vele.
- Bármely adatkezelést végző szervezeti egység szakterületi vezetőjének kérésére véleményezi a NAIH-nak címzett, hivatalos megkereséseket és egyéb dokumentumokat.
- Ha felmerül az adatvédelmi előírások megszegése, illetve a rendszerbe épített védelmi eljárások működési hibája, intézkedik a rendszer felülvizsgálata érdekében, emberi mulasztás esetén kezdeményezi a tényleges helyzet feltárását és értékelését.
- A Társaságnál használt, személyes adatokat tároló, kezelő, feldolgozó informatikai rendszerekben történő jogosultság-változások kapcsán, adatvédelmi-adatbiztonsági probléma felmerülése esetén, tájékoztatja a jogi és humánpolitikai, valamint a biztonsági igazgatót, továbbá az informatikai főosztályvezetőt.
- Elkészíti és aktualizálja a Társaság egészére vonatkozó adatvédelmi és adatbiztonsági szabályokat.
- Elérhetővé teszi az adatkezelést végző szervezeti egységek X.3. pontban foglaltak szerint kijelölt munkavállalói részére az adatkezelést végző szervezeti egységek feladatainak teljesítéséhez felhasználható dokumentumokat, mintákat és formanyomtatványokat, valamint az adatkezelések nyilvántartását tartalmazó felületet. Az adatkezelést végző szervezeti egységek hivatkozott munkavállalóinak kezdeményezésére az adott szervezeti egységek további munkavállalóinak is biztosíthatja a hozzáférést. A kezdeményezés indokoltságáért a kezdeményező felel.
- Ellátja a Rendeletben számára meghatározott egyéb feladatokat.

3. Az adatvédelmi tisztviselő jogai

- Az ellenőrzött területre, illetve bármely helyiségbe, létesítménybe, ahol adatkezelés folyik, beléphet.[10]
- Az ellenőrzés során betekintése van minden munkafolyamatba, dokumentumba, mely az adatvédelemmel és adatbiztonsággal kapcsolatban áll. Igényelhet minden adatvédelemhez és adatbiztonsághoz kapcsolódó információt. Jogosult teljes mélységben betekinteni a személyes adatkezelések anyagaiba, teljes körű tájékoztatást kapni a vizsgált adatkezelésekről, minden olyan adatkezelést megismerni, amely személyes vagy közérdekű adatokkal összefügghet.
- A megtekintett dokumentumokról, bizonylatokról másolatot, kivonatot, tanúsítványt készíthet vagy kérhet. Súlyos szabálytalanság, visszaélés felmerülése esetén a bizonyítás szempontjából fontos irat meghamisításának vélelme esetén az eredeti bizonylatot is lefoglalhatja, és magával viheti.[11]
- Az ellenőrzéssel kapcsolatban bármely munkavállalótól szóbeli felvilágosítást vagy írásbeli nyilatkozatot kérhet. A felvilágosítást mindenki köteles megadni, függetlenül a beosztásától vagy attól, hogy az ellenőrzés mely szervnél folyik. Ehhez a munkavállalónak felettesétől nem kell előzetesen engedélyt kérni. A felvilágosítás megtagadására utasítást beosztottak részére vezetők nem adhatnak.

[10] Az erre vonatkozó külön szabályok figyelembevételével.

[11] Másolat visszahagyása mellett.

- Írásbeli nyilatkozatok, papíralapú vagy elektronikus levél formájában történt megkeresésekre az adatvédelmi tisztviselő válaszadási határidőt jelölhet ki.
- Az ellenőrzéssel kapcsolatban a bizonylatok valódiságának ellenőrzése vagy az adatok kiegészítése céljából az adatvédelmi tisztviselő külső szerveket is megkereshet.[12]
- Az adatvédelmi tisztviselő részére teljes betekintési (olvasási) jog a Társaságnál használt rendszer HR moduljába célellenőrzéshez adható, a HR felelős előzetes tájékoztatását követően.
- Az adatvédelmi tisztviselő az adatvédelmi ellenőrzések kapcsán felmerülő, a Társaságnál használt informatikai rendszerekhez szükséges (ideiglenes) jogosultság-igények soron kívüli, legrövidebb időn belüli beállítását kérheti.
- Tájékoztatást kérhet bármely, a Társaságnál használt informatikai rendszerekben történő jogosultság-módosításokkal kapcsolatosan.

Szükség esetén (ha adatvédelmi szempontok megkívánják) az adatvédelmi tisztviselő kifejtheti szakmai álláspontját a rendszergazdai, illetőleg HR modulban történt bármely jogosultság-módosításokkal kapcsolatosan, melyet a technikai lehetőségek határáig figyelembe kell venni.

4. Az adatvédelmi tisztviselő kötelességei

Az adatvédelmi tisztviselő köteles különösen:

- a Szabályzat aktualizálását az előírtaknak megfelelően kezdeményezni,
- a NAIH-nak küldendő éves jelentés határidőre történő megküldéséről intézkedni,
- a Társaság adatvédelmi nyilvántartását az előírtaknak megfelelően aktualizálni,
- a Társaság munkavállalói vonatkozásában az adatvédelmi és adatbiztonsági tevékenység során az elvárható legnagyobb gondossággal eljárni,
- az adatvédelmi ellenőrzésekre megfelelően felkészülni, azok lebonyolítását megszervezni,
- a vizsgált szervezeti egység vezetőjénél bejelenteni a helyszíni ellenőrzés megkezdését,
- a feltárt súlyos hiányosságokért felelős személy(eke)t megnevezni,
- a felelősként megjelölt személlyel a megállapításait írásban ismertetni, és tőle írásbeli magyarázatot kérni,
- a felelősként megjelölt személy írásbeli magyarázatában foglaltak elfogadásáról vagy elutasításáról írásban nyilatkozni,
- az adatvédelmi ellenőrzésről jelentést készíteni és a megállapítások tartalmát az ellenőrzött szervezeti egység vezetőjével, valamint az érdekeltekkel ismertetni,
- az ellenőrzés lezárásakor az adatvédelmi ellenőrzési jelentés egy példányát az ellenőrzött szervezeti egység vezetőjének – és szükség szerint az adatkezelést végző szervezeti egység vezetőjének – átadni,
- az adatvédelmi ellenőrzés megállapításaira adott jelentéseket értékelni,
- az adatvédelmi ellenőrzéssel kapcsolatos kötelességekre az ellenőrzött munkavállalók figyelmét felhívni és jogaikról tájékoztatni,
- jogviszonyának fennállása alatt és annak megszűnését követően is titokként megőrizni a tevékenységével, annak ellátásával kapcsolatban tudomására jutott személyes adatot,

[12] Külön ügyvezetői engedéllyel.

illetve törvény által védett titoknak és hivatás gyakorlásához kötött titoknak minősülő adatot, valamint minden olyan adatot, tényt vagy körülményt, amelyet Társaságunk vagy adatfeldolgozó nem köteles törvény előírásai szerint a nyilvánosság számára hozzáférhetővé tenni.

5. Az adatvédelmi tisztviselő felelőssége

Az adatvédelmi tisztviselő munkavégzése során felelős:

- a bejelentések kapcsán beérkező információk bizalmas kezeléséért,
- az adatvédelmi ellenőrzésről készített jelentés előírt határidőre történő elkészítéséért,
- a Társaság munkavállalói vonatkozásában az adatvédelmi és adatbiztonsági tevékenység ellenőrzéséért,
- az adatvédelmi ellenőrzések során tett megállapítások helyességéért és előírásszerű bizonyításáért.

VII. FEJEZET

AZ ADATVÉDELMI ELLENŐRZÉSBEN ÉRINTETTEK JOGAI, KÖTELEZETTSÉGEI ÉS FELELŐSSÉGE

Az adatvédelmi ellenőrzés alapvetően az éves adatvédelmi ellenőrzési terven alapul Ezen kívül alapulhat ügyvezetői, valamint az adatvédelmi tisztviselő által kezdeményezett — eseti, bejelentéseken alapuló — elrendelésen (eseti elrendelés) is.

1. Az adatvédelmi ellenőrzésben érintett szervezet vezetőinek és munkavállalóinak kötelessége

Az adatvédelmi ellenőrzésben érintett vezetők és munkavállalók kötelesek:

- biztosítani az ellenőrzés zökkenőmentes, zavartalan lebonyolításához szükséges feltételeket,
- lehetővé tenni a különféle dokumentumokba való betekintést, a helyiségekbe való bejutást,
- az adatvédelmi tisztviselő által feltett kérdésekre a valós tényeknek megfelelően szóban vagy írásban nyilatkozni,
- az adatvédelmi tisztviselő megkeresésében kijelölt válaszadási határidőn belül válaszát a felelőshöz eljuttatni,
- elősegíteni a tapasztalható hibák, mulasztások teljes körű feltárását, illetve keletkezésük valódi okainak megismerését,
- az adatvédelmi tisztviselő írásos felhívására az általa megjelölt határidőn belül (legkevesebb 3 munkanap) írásbeli magyarázatot adni a megállapított hibákat előidéző okokról és a vizsgálat ideje alatt ezek megszüntetésére tett intézkedésekről,
- az ellenőrzés során feltárt, az ellenőrzésben érintett szervezet hatáskörébe tartozó szabálytalanságok, hibák, mulasztások haladéktalan megszüntetéséről gondoskodni,
- az ellenőrzésről szóló jelentés átvételét követően szabálytalanságokat, hibákat, mulasztásokat elkövető munkavállalókat felelősségre vonni, figyelemmel a jogszabályokban (Ptk., Mt.) meghatározott jogvesztő határidőkre,
- a hiányosságok, szabálytalanságok ismétlődése esetén az ellenőrzött szervezeti egység(ek) vezetőjének felelősségre vonását kezdeményezni.

2. Az adatvédelmi ellenőrzésben érintett szervezet vezetőinek és munkavállalóinak jogai

Az adatvédelmi ellenőrzésben érintett vezetők és munkavállalók jogosultak arra, hogy:

- meggyőződhessenek az ellenőrzés jogszerűségéről,
- megismerjék az ellenőrzésről szóló jelentés megállapításait,
- észrevételt tegyenek az átadott jelentésben foglalt megállapításokra, és észrevételeikre választ kapjanak,
- az ellenőrzés során az általuk lényegesnek ítélt szempontokra az adatvédelmi tisztviselő figyelmét felhívják,

- személyiségi jogaikat sértő kérdésekben a válaszadást megtagadják (a személyiségi jog sérülésével kapcsolatos vita esetén a jogi és humánpolitikai igazgató állásfoglalását kell kérni).

3. Az adatvédelmi ellenőrzést kezdeményező vezető kötelessége

Az adatvédelmi ellenőrzést kezdeményező vezető a megállapított tények minősítése alapján köteles:

- bűncselekmény gyanúja esetén további bizonyítékokat beszerezni, konzultálni az illetékes (nem érintett) vezetőkkel, illetve szakértőkkel és jogászokkal,
- bűncselekmény alapos gyanúja esetén — konzultálást követően — büntető feljelentést tenni, illetőleg azt kezdeményezni,
- munkafegyelmi vétség esetén fegyelmi felelősségre vonást elrendelni vagy kezdeményezni a mulasztást, illetve kárt okozóval szemben a munkáltatói jogkör gyakorlójánál,
- hiányosság előfordulása esetén felszólítani a hibázó(ka)t, hogy tegyen(ek) javaslatot az előfordulás megakadályozására,
- az ügyet lezárni, amennyiben az ellenőrzés semmilyen lényeges észrevételt nem tett.

Az ellenőrzést kezdeményező vezető kezdeményezése alapján a munkáltatói jogkör gyakorlója köteles a fegyelmi eljárást lefolytatni, és annak eredményéről az ellenőrzést végzőt a kezdeményezés kézhezvételétől számított legkésőbb 60 napon belül írásban tájékoztatni.
A fegyelmi eljárás lefolytatásán kívül meg kell tenni a szükséges intézkedéseket az ismétlődés lehetőségének megakadályozására.
Ha a munkáltatói jogkör gyakorlója az előzőekben leírtak szerinti kötelességének nem tesz eleget, az ellenőrzést végző szerv vezetője köteles erről a munkáltatói jogkör gyakorlójának felettesét értesíteni.
Az ügyvezető által elrendelt eseti ellenőrzés esetén jelen pontban meghatározott intézkedéseket a az ügyvezető által megbízott vezető végzi el.

VIII. FEJEZET

AZ ADATKEZELÉSI TEVÉKENYSÉGEK NYILVÁNTARTÁSA

Társaságunk a felelősségébe tartozóan végzett adatkezelési tevékenységekről köteles nyilvántartást vezetni.

E nyilvántartás a következő információkat tartalmazza:

a) az adatkezelő neve és munkahelyi elérhetősége, valamint – ha van ilyen – a közös adatkezelőnek, az adatkezelő képviselőjének és az adatvédelmi tisztviselőnek a neve és munkahelyi elérhetősége;
b) az adatkezelés célja(i);
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 továbbítás esetében a megfelelő garanciák leírása;
f) ha lehetséges, a különböző adatkategóriák törlésére előirányzott határidők;
g) ha lehetséges, az adatbiztonságot érintő technikai és szervezési intézkedések általános leírása.

Amennyiben Társaságunk valamely jogviszonyban adatfeldolgozó köteles nyilvántartást vezetni az adatkezelő nevében végzett adatkezelési tevékenységek minden kategóriájáról; a nyilvántartás a következő információkat tartalmazza:

a) az adatfeldolgozó vagy adatfeldolgozók neve és munkahelyi elérhetőségei, és minden olyan adatkezelő neve és elérhetőségei, amelynek vagy akinek a nevében az adatfeldolgozó eljár, továbbá – ha van ilyen – a Társaságunk vagy az adatfeldolgozó képviselőjének, valamint az adatvédelmi tisztviselőnek a neve és elérhetőségei;
b) az egyes adatkezelők nevében végzett adatkezelési tevékenységek kategóriái;
c) adott esetben a személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítása, beleértve a harmadik ország vagy a nemzetközi szervezet azonosítását, valamint továbbítás esetében a megfelelő garanciák leírása;
d) ha lehetséges, a technikai és szervezési intézkedések általános leírása.

A nyilvántartás vezetéséről – a társasági Ügyrend szerinti feladataik alapulvételével – az adatkezelést végző szervezeti egységek vezetői kötelesek gondoskodni. A nyilvántartást írásban, az adatvédelmi tisztviselő útmutatása szerint kialakított adattartalommal kell vezetni és azt a társasági szintű összesített nyilvántartás érdekében az adatvédelmi tisztviselőnek kell megküldeni.

Az adatkezelésért felelős szervezeti egységek vezetői kötelesek az adatkezelés változása esetén (Pl. új vagy megszűnő feladat kapcsán) gondoskodni a nyilvántartásuk frissítéséről, továbbá a frissítést megelőzően az előző időállapot szerinti nyilvántartások megőrzéséről oly módon, hogy a változások időpontja követhető legyen. A változásról a frissítést követően a frissített nyilvántartás megküldésével haladéktalanul tájékoztatni kell az adatvédelmi tisztviselőt is.

Ezen túlmenően az adatkezelésért felelős szervezeti egységek vezetői kötelesek minden év március 31. napjáig gondoskodni a nyilvántartásuk felülvizsgálatáról- és az adatvédelmi tisztviselő a fentiek szerinti tájékoztatásáról az esetleges módosulásokról vagy arról, hogy a nyilvántartásuk nem módosult.

Társaságunk megkeresés alapján köteles a NAIH részére rendelkezésre bocsátani a nyilvántartást.

IX. FEJEZET

ADATVÉDELMI HATÁSVIZSGÁLAT ÉS ELŐZETES KONZULTÁCIÓ

Ha 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, akkor Társaságunk az adatkezelést megelőzően hatásvizsgálatot végez arra vonatkozóan, hogy a tervezett adatkezelési műveletek a személyes adatok védelmét hogyan érintik.

Ha a NAIH valamely meghatározott adatkezelés-típust magas kockázatú adatkezelésnek minősít és e megállapítását közzéteszi, valamint a tervezett adatkezelés e megállapítással érintett adatkezelés-típus során alkalmazottal azonos vagy ahhoz hasonló típusú művelet vagy műveletsorozat alkalmazásával jár, a tervezett adatkezelés tekintetében annak magas kockázatát vélelmezni kell.

Ha a NAIH valamely meghatározott adatkezelés-típus tekintetében azt állapítja meg, hogy az nem minősül magas kockázatú adatkezelésnek és e megállapítását közzéteszi, valamint a tervezett adatkezelés kizárólag e megállapítással érintett adatkezelés-típus során alkalmazottal azonos vagy ahhoz hasonló típusú művelet vagy műveletsorozat alkalmazásával jár, a tervezett adatkezelés tekintetében azt kell vélelmezni, hogy az nem minősül magas kockázatú adatkezelésnek.

Kötelező adatkezelés esetén az adatvédelmi hatásvizsgálatot az adatkezelést előíró jogszabály előkészítője folytatja le.

Olyan egymáshoz hasonló típusú adatkezelési műveletek, amelyek egymáshoz hasonló magas kockázatokat jelentenek, egyetlen hatásvizsgálat keretei között is értékelhetők.

Az adatvédelmi hatásvizsgálat elvégzéséről és aktualizálásáról az adatkezelést végző szervezeti egység vezetője köteles gondoskodni.

Az adatvédelmi hatásvizsgálat elvégzésekor az adatvédelmi tisztviselő szakmai tanácsát kötelező kikérni.

Az adatvédelmi hatásvizsgálatot különösen az alábbi esetekben kell elvégezni:

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) a személyes adatok különleges kategóriái, vagy a büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó személyes adatok nagy számban történő kezelése; vagy
c) nyilvános helyek nagymértékű, módszeres megfigyelése.

A hatásvizsgálat kiterjed legalább:

a) a tervezett adatkezelési műveletek módszeres leírására és az adatkezelés céljainak ismertetésére, beleértve adott esetben a Társaságunk által érvényesíteni kívánt jogos érdeket;
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.

Előzetes konzultáció:

Ha a fentiekben előírt adatvédelmi hatásvizsgálat megállapítja, hogy az adatkezelés a Társaságunk által a kockázat mérséklése céljából tett intézkedések hiányában valószínűsíthetően magas kockázattal jár, a személyes adatok kezelését megelőzően Társaságunk köteles konzultálni NAIH-al.

Kötelező adatkezelés esetén az előzetes konzultációt az adatkezelést előíró jogszabály előkészítője a jogszabály-előkészítési eljárás keretei között kezdeményezi és folytatja le.

X. FEJEZET

RENDELKEZŐ RÉSZ

1. A telephelyeken folyó adatkezelések részletes szabályainak kidolgozása, naprakészen tartása a vonatkozó jogszabályok és jelen Szabályzat előírásai alapján, különös tekintettel a személyes adatokkal kapcsolatos jogok érvényesítésének, illetve a közérdekű adatok kiadásának rendjére.

   Határidő: folyamatos, a személyes adatok megismerésének rendjére vonatkozóan a Szabályzat hatálybalépését követő 30. nap, illetve folyamatos
   Felelős: adatkezelést végző szervezeti egységek vezetői

2. A hatályos társasági szabályozások adatvédelmet érintő rendelkezéseinek felülvizsgálata, szükség esetén azok módosítása a Rendeletnek és jelen Szabályzatnak megfelelően.

   Határidő: a Szabályzat hatálybalépését követő 45. nap
   Felelős: adatkezelést végző szervezeti egységek vezetői

3. Azon munkavállaló kijelölése, nevének, elérhetőségeinek megküldése az adatvédelmi tisztviselő felé, aki az adott szervezeti egységen belül koordinálja és az érintettek, a hatóságok, illetve harmadik személyek és szervek irányában biztosítja az adatvédelemmel kapcsolatban jelen Szabályzatban meghatározott vagy egyébként a mindenkor hatályos jogszabályok alapján felmerülő kötelezettségek teljesítését.

   Határidő: a Szabályzat hatálybalépését követő 15. nap
   Felelős: adatkezelést végző szervezeti egységek vezetői

4. A közös adatkezelésre tekintettel vagy adatfeldolgozó igénybevétele esetén a Rendelet követelményeinek érvényesítése a szerződésekben.

   Határidő: a már megkötött szerződések esetén a Szabályzat hatályba lépését követő 30. nap, egyébként a szerződés megkötésének előkészítése során folyamatos
   Felelős: adatkezelést végző szervezeti egységek vezetői

5. Az adatkezelések nyilvántartásának vezetése és adatszolgáltatás a társasági szintű nyilvántartáshoz az adatvédelmi tisztviselő részére.

   Határidő: a Szabályzat hatályba lépését követően, valamint változás esetén haladéktalanul, illetve minden év március 31. napjáig
   Felelős: adatkezelést végző szervezeti egységek vezetői

6. Adatvédelmi hatásvizsgálat lefolytatása a Rendeletben meghatározott esetekben.

Határidő: a hatásvizsgálati kötelezettség alá tartozó új adatkezelés megkezdését megelőzően; valamint haladéktalanul abban az esetben, amennyiben a folyamatban lévő adatkezelés körülményeiben a Rendelet alkalmazandóságának időpontját követően jelentős változás áll be
Felelős: adatkezelést végző szervezeti egységek vezetői

7. Valamennyi, a Társaság kezelésében/tulajdonában, stb. lévő kameráról nyilvántartás készítése és vezetése, elkülönítve a Kivételi Körbe tartozó kamerákat azoktól, melyekkel adatkezelés valósul meg, illetve elkülönítve a telephelyi (tehát munkavállalókat), illetve vagyonvédelmi stb. (tehát elsődlegesen területet) megfigyelő kamerákat.

Határidő: folyamatos
Felelős: adatkezelést végző szervezeti egységek vezetői

8. A személyes adatok kezelésére vonatkozó tájékoztatás megvalósítása, hozzájárulások beszerzése.

Határidő: a folyamatban lévő adatkezelések esetén a Szabályzat hatálybalépését követő 30. nap, egyébként folyamatos
Felelős: adatkezelést végző szervezeti egységek vezetői

9. Jelen Szabályzat évente történő felülvizsgálata, a felülvizsgálat eredményétől függően a Szabályzat módosításának kezdeményezése.

Határidő: minden év január 31.
Felelős: adatvédelmi tisztviselő

10. Az adatvédelemmel összefüggő oktatások megszervezése, lebonyolítása, az adatvédelmi tisztviselővel együttműködve.

Határidő: folyamatos
Felelős: ügyvezető igazgató

11. Az informatikai rendszerekben kezelt személyes adatok törléséhez szükséges folyamatok, automatizmusok kialakításának biztosítása a szakterületek részére.

Határidő: folyamatos
Felelős: ügyvezető

A Szabályzattal kapcsolatban felvilágosítást adatvédelmi kérdésekben az adatvédelmi tisztviselő ad a 06204599225-ös telefonszámon.

Budapest, 2018. július 30. napja

Kálmán Zsolt
ügyvezető

TITOKTARTÁSI NYILATKOZAT

Alulírott: .....

tudomásul veszem, hogy a BKV Panoráma Kft. tevékenységével kapcsolatban, a munkavégzésem során szóban, írásban, bármely informatikai rendszerből vagy egyéb módon tudomásomra jutott információt, adatot köteles vagyok megőrizni, ezen információk jogosulatlan felhasználása, illetéktelen személy részére történő hozzáférhetővé tétele munkajogi, polgári- és büntetőjogi jogkövetkezményeket vonhat maga után.

Kelt: ……, ……

.....
(név)
(munkakör)
nyilatkozatot tevő/munkavállaló

Kelt: ……, ……

.....
(név)
(munkakör)
munkáltatói jogkörgyakorló

JEGYZŐKÖNYV

MEGKERESÉS ALAPJÁN AZ EURÓPAI UNIÓN BELÜL TELJESÍTETT ADATTOVÁBBÍTÁSRÓL

(beleértve a belföldre irányuló adattovábbításokat)

1. A megkeresést végző szerv vagy személy

megnevezése: ……

postacíme: …….

telefonszáma: ……..

e-mail: ……..

2. Az adatkérés

célja: ……..

rendeltetése: ……

jogszabályi alapja: ……

illetve az érintett hozzájáruló nyilatkozata ☐

időpontja: ……

3. Az adatszolgáltatás alapjául szolgáló

adatkezelés megnevezése: ……..

4. **Az adatszolgáltatást teljesítő**

szervezeti egység neve: ……..

vezetőjének neve, munkaköre: ……

5. Az érintettek

köre: ……

6. A továbbított adatok

köre: ……

7. Az adattovábbítás

módja: ……

Kelt: ……, ……

…….
(név)
(munkakör)

JEGYZŐKÖNYV

EURÓPAI UNIÓN KÍVÜLI ORSZÁGBA VAGY NEMZETKÖZI SZERVEZET RÉSZÉRE TÖRTÉNŐ ADATTOVÁBBÍTÁSRÓL

1. **Az adattovábbítás címzettje**

megnevezése: ……

postacíme: …….

telefonszáma: ……..

e-mail: ……..

2. Az adattovábbítás

célja:

rendeltetése: ……

jogszabályi alapja: ……

illetve az érintett hozzájáruló nyilatkozata ☐

időpontja: ……

3. Az adatszolgáltatást teljesítő

szervezeti egység neve: ……..

vezetőjének neve, beosztása: ……

4. Az érintettek

köre: ……

5. A továbbított adatok

köre: ……

6. Az adattovábbítás

módja: ……

7. Az adattovábbítás

garanciái: ……

Kelt: ……, ……

…….
(név)
(munkakör)