

Társasági Adatvédelmi és Adatbiztonsági SZABÁLYZAT

2016.

TARTALOMJEGYZÉK

Tartalomjegyzék	2
Bevezetés	5
I. FEJEZET Általános rendelkezések	6
1. A Szabályzat célja és hatálya	6
a) Személyi hatály.....	6
b) Tárgyi hatály.....	6
2. A Szabályzat aktualizálása	7
II. FEJEZET Az adatvédelemre vonatkozó rendelkezések	8
1. A Társaságnál kezelt adatok osztályozása	8
a) Személyes adat.....	8
b) Különleges adat.....	8
c) Minősített adat (a minősített adat védelméről szóló 2009. évi CLV. tv. alapján).....	8
d) Magántitok, levéltitok.....	9
e) Üzleti titok	9
2. Az adatokhoz tartozó adatvédelmi kategóriák	9
a) Alap biztonsági szint.....	9
b) Megemelt biztonsági szint	9
c) Fokozott biztonsági szint.....	10
d) Kiemelt biztonsági szint.....	10
3. Az egyes adatkezelő szervezeti egységek biztonsági besorolása.....	10
4. Az egyes adatkezelő szervezeti egységek feladatai	10
5. A Társaság adatvagyonát érintő események	11
III. FEJEZET A személyes adatok kezelésére vonatkozó szabályok	12
1. A személyes adat kezelésének célhoz kötöttsége.....	13
2. A személyes adat kezelésének társasági szabályai	13
a) Személyazonosító adatok kezelése	13
b) Munkabér, egyéb járandóság, illetőleg a munkaviszony kapcsán keletkező adatok kezelése	14
c) Videómegfigyelő-rendszerek működtetése.....	15
d) A forgalmi üzemeltetés során végzett hangrögzítés.....	22
e) Az adatkezelések törzskönyve	23
3. Adatok minőségi követelményei.....	23
4. Adatközlések	24
a) Személyes adat nyilvánosságra hozatala.....	24
b) Adatkezelések összekapcsolása	24
c) Belföldre irányuló adattovábbítások.....	24
d) Külföldre irányuló adattovábbítások.....	25
5. Érintettek jogai és érvényesítésük	25
a) Tájékoztatásra, illetve betekintésre irányuló kérelem	25
b) Tájékoztatásra, illetve betekintésre irányuló kérelem megtagadása	26

c) Személyes adat helyesbítése, törlése, megjelölése, illetve zárolása	27
6. Adatfeldolgozó igénybevételek szabályai	28
a) Az adatkezelő felelőssége.....	28
b) Az adatfeldolgozó felelőssége	28
IV. FEJEZET A közérdekű adatok nyilvánosságára vonatkozó előírások	30
V. FEJEZET Az adatvédelem és adatbiztonság technikai hátterének egyes kérdései,	
IRATMINŐSÍTÉSI ALAPELVEK	33
1. Az infrastruktúrához kapcsolódó védelmi intézkedések	33
a) Szervertermek üzemeltetési rendje, biztonsági előírásai	33
b) Informatikai rendszerek osztályozási irányelvei.....	33
c) Az információs vagyonelemek osztályozása	37
2. Eseti biztonsági intézkedések.....	37
3. A hardverekhez kapcsolódó védelmi intézkedések	37
4. A szoftverekhez kapcsolódó védelmi intézkedések	37
A szoftverekhez kapcsolódó védelmi intézkedések részletes rendjét az Informatikai Biztonsági Szabályzat tartalmazza.	38
5. Katasztrófhelyzetek kezelése	38
6. Az adathordozókhoz kapcsolódó védelmi intézkedések	38
7. Az információ kezelésével kapcsolatos intézkedések	38
VI. FEJEZET Az adatvédelmi felelős feladatai, jogai, kötelezettségei és felelőssége	40
1. Az adatvédelmi felelős Infotv.-ben meghatározott feladatai	40
2. Az adatvédelmi felelős további, társasági szempontból lényeges feladatai	40
3. Az adatvédelmi felelős jogai.....	41
4. Az adatvédelmi felelős kötelezettségei	42
5. Az adatvédelmi felelős felelőssége	42
VII. FEJEZET Az adatvédelmi ellenőrzésben érintettek jogai, kötelezettségei és felelőssége	43
1. Az adatvédelmi ellenőrzésben érintett szervezet vezetőinek és munkavállalóinak kötelessége.....	43
2. Az adatvédelmi ellenőrzésben érintett szervezet vezetőinek és munkavállalóinak jogai	43
3. Az adatvédelmi ellenőrzést elrendelő vezető kötelessége	44
VIII. FEJEZET Az adatvédelmi nyilvántartás	45
1. Bejelentkezés a nyilvántartásba	45
2. Új adatállomány feldolgozása	46
IX. FEJEZET Rendelkező rész	47
TÖRZSKÖNYV.....	51
JEGYZŐKÖNYV	53
JEGYZŐKÖNYV	54
JEGYZŐKÖNYV	55

1. Függelék Kapcsolódó jogszabályok gyűjteménye	56
2. Függelék Fogalmak.....	57

BEVEZETÉS

Az információs önrendelkezési jogról és az információszabadságról szóló **2011. évi CXII. törvény (a továbbiakban: Infotv.) előírja, hogy** az országos hatósági, munkaügyi vagy bűnügyi adatállományt kezelő, illetőleg feldolgozó adatkezelőknek és adatfeldolgozóknak adatvédelmi és adatbiztonsági szabályzatot (a továbbiakban: Szabályzat) kell készíteniük. Fenti törvény kötelezettséget ró a Budapesti Közlekedési Zártkörűen Működő Részvénytársaságra (a továbbiakban: Társaság), mint adatkezelőre, hogy az adatkezelő szerv vezetőjének felügyelete alá tartozó — jogi, közigazgatási, számítástechnikai vagy ezeknek megfelelő, felsőfokú végzettséggel rendelkező — belső **adatvédelmi felelőst kell kinevezni**, akinek feladata a belső adatvédelmi és adatbiztonsági szabályzat elkészítése mellett az Infotv. 24. § (2) bekezdésében, illetve a jelen Szabályzat VI. fejezetet 2. pontjában meghatározott feladatok ellátása.

Az Infotv. rendelkezéseinek végrehajtása érdekében, valamint az Európai Unióhoz történt csatlakozás kapcsán a Társaságot érintő adatkezelésekre, adatvédelmi és adatbiztonsági feladatokra történő felkészülés érdekében, a következők szerint rendelkezem.

I. FEJEZET

ÁLTALÁNOS RENDELKEZÉSEK

1. A Szabályzat célja és hatálya

Jelen Szabályzat célja, hogy meghatározza a Társaság adatkezelésének és az adatok nyilvántartásának, védelmének törvényes rendjét, valamint biztosítsa az adatvédelem alkotmányos elveinek, az információs önrendelkezési jognak és az adatbiztonság követelményeinek érvényesülését.

Fentiek teljesülése érdekében jelen Szabályzat a Társaság információvédelmi szabályozási struktúrájának tetején foglal helyet; a szabályozási struktúra további elemei:

- Informatikai Biztonsági Szabályzat,
- Iratkezelési Szabályzat,
- Biztonsági és Vagyonvédelmi Szabályzat,
- Közzétételi Szabályzat,
- Minősített Iratok Társasági Kezelésének Szabályozása,
- Vagyonnyilatkozat-tételi Szabályzat.

A Szabályzat rendelkezéseit figyelembe kell venni a Társaságnál kiadásra kerülő szabályozásoknál, illetve meglévő (hatályos) szabályozások módosításakor.

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 a számítástechnika-alkalmazás, szoftverfejlesztés és iratkezelés teljes folyamatára. Kiterjed továbbá valamennyi, a Társaságnál kezelt természetes személy adatára, közérdekű, illetve közérdekből nyilvános adatra — függetlenül annak előállítási vagy feldolgozási módjától és megjelenési formájától — és magára az adatkezelésre is.

2. A Szabályzat aktualizálása

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

- ha a Társaság adatvédelmét, illetve a társasági Adatvédelmi és Adatbiztonsági 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.

II. FEJEZET

AZ ADATVÉDELEMRE VONATKOZÓ RENDELKEZÉSEK

1. A Társaságnál kezelt adatok osztályozása

a) Személyes adat

Bármely meghatározott (azonosított vagy azonosítható) természetes személlyel (a továbbiakban: érintett) kapcsolatba hozható adat - különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret -, az adatból levonható, az érintettre vonatkozó következtetés. A személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel helyreállítható¹.

b) Különleges adat

- ba) A faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdekképviseleti szervezeti tagságra, a szexuális életre vonatkozó személyes adat,
- bb) az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat, valamint a bűnügyi személyes adat.

c) Minősített adat (a minősített adat védelméről szóló 2009. évi CLV. tv. alapján)

- ca) *nemzeti minősített adat*: a minősítéssel védhető közérdekek körébe tartozó, a minősítési jelölést („Szigorúan titkos!”, „Titkos!”, „Bizalmas!”; és „Korlátozott terjesztésű!”) a minősített adat védelméről szóló 2009. évi CLV. törvényben, valamint a törvény felhatalmazása alapján kiadott jogszabályokban meghatározott formai követelményeknek megfelelően tartalmazó olyan adat, amelyről - a megjelenési formájától függetlenül - a minősítő a minősítési eljárás során megállapította, hogy az érvényességi időn belüli nyilvánosságra hozatala, jogosulatlan megszerzése, módosítása vagy felhasználása, illetéktelen személy részére hozzáférhetővé, valamint az arra jogosult részére hozzáférhetetlenné tétele a minősítéssel védhető közérdekek közül bármelyiket közvetlenül sérti vagy veszélyeztet, és tartalmára tekintettel annak nyilvánosságát és megismerhetőségét a minősítés keretében korlátozza;
- cb) *külföldi minősített adat*: az Európai Unió valamennyi intézménye és szerve, továbbá az Európai Unió képviselőjében eljáró tagállam, a külföldi részes fél vagy nemzetközi szervezet által készített és törvényben kihirdetett nemzetközi szerződés vagy megállapodás

¹ Az érintettel akkor helyreállítható a kapcsolat, ha az adatkezelő rendelkezik azokkal a technikai feltételekkel, amelyek a helyreállításához szükségesek.

alapján átadott olyan adat, amelyhez történő hozzáférést az Európai Unió intézményei és szervei, az Európai Unió képviseletében eljáró tagállam, más állam vagy külföldi részes fél, illetve nemzetközi szervezet minősítés keretében korlátozza;

d) 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.

e) Üzleti titok

A Ptk-ban foglalt főszabály szerint üzleti a gazdasági tevékenységhez kapcsolódó minden nem közismert vagy az érintett gazdasági tevékenységet végző személyek számára nem könnyen hozzáférhető olyan tény, tájékoztatás, egyéb adat és az azokból készült összeállítás, amelynek illetéktelenek által történő megszerzése, hasznosítása, másokkal való közlése vagy nyilvánosságra hozatala a jogosult jogos pénzügyi, gazdasági vagy piaci érdekét sértene vagy veszélyeztetné, feltéve, hogy a titok megőrzésével kapcsolatban a vele jogszerűen rendelkező jogosultat felróhatóság nem terheli.

Nem minősül üzleti titoknak az állami és a helyi önkormányzati költségvetés, illetve az európai közösségi 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 technológiai eljárásokra, a műszaki megoldásokra, a gyártási folyamatokra, a munkaszervezési és logisztikai módszerekre, továbbá a know-how-ra vonatkozó adatokhoz - való hozzáférést, amelyek megismerése az üzleti tevékenység végzése szempontjából aránytalan sérelmet okozna, feltéve, hogy ez nem akadályozza meg a közérdekből nyilvános adat megismerésének lehetőségét.**

2. Az adatokhoz tartozó adatvédelmi kategóriák

Az adatok kezelését a következő fokozatokban lehet megvalósítani a nyilvántartások, adatbázisok esetében.

a) Alap biztonsági szint

A biztonság szempontjából minden olyan adat, amely nem igényel magasabb besorolást, és a többi adatvédelmi kategóriába nem sorolható be, alap biztonsági fokozatú.

b) Megemelt biztonsági szint

A biztonság szempontjából a személyes adatok, üzleti titkot képező (bizalmas) adatok, valamint minden más, a Társaság tevékenysége során tudomására jutott titok — így például magántitok, üzleti titok — besorolása megemelt biztonsági fokozatú.

c) Fokozott biztonsági szint

Ebbe a szintbe kell besorolni az olyan, egyedileg nem minősített, különleges adatokat, amelyek egyesített megjelenései fokozott védelmet igényelnek.

d) Kiemelt biztonsági szint

Amennyiben minősített adatokat is tartalmaz a szervezet adatkezelése — kiemelt biztonsági besorolás mellett — a minősített adat védelméről szóló 2009. évi CLV. tv. vonatkozó rendelkezései az irányadók.

3. Az egyes adatkezelő szervezeti egységek biztonsági besorolása

A Társaság által kezelt adatok biztonsági fokozata szerint az egyes adatkezelő szervezeti egységek adatvédelmi és adatbiztonsági szempontú biztonsági besorolását az adatvédelmi felelős az adatkezelést végző szervezeti egység vezetőjével egyetértésben állapítja meg, a következők szerint.

Az alap biztonsági fokozatba tartozik valamennyi szervezeti egység.

A megemelt biztonsági fokozatba tartozik az a szervezeti egység, amely személyes adatok, üzleti titkot képező (bizalmas) adatok, valamint minden más, a Társaság tevékenysége során tudomására jutott titkokat — így például magántitok, üzleti titok — kezel.

Fokozott biztonsági fokozatba tartozik az a szervezeti egység, amely olyan, egyedileg nem minősített, különleges adatokat kezel, amelyek egyesített megjelenései fokozott védelmet igényelnek.

A minősített adat védelméről szóló 2009. évi CLV. tv. szerinti minősített adatokat kezelő szervezeti egységek a *kiemelt biztonsági fokozatba* tartoznak.

A minősítésnek az adatvédelem és adatbiztonság érdekében alkalmazott intézkedések szempontjából van jelentősége.

4. Az egyes adatkezelő szervezeti egységek feladatai

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 az Infotv-ben meghatározott feladatok, kötelezettségek ellátásáról, különös tekintettel az érintettek jogainak védelmére, tájékoztatásukra.

5. A Társaság adatvagyonát érintő események

A Társaság adatvagyonát érintő rendkívüli adatvédelmi esemény kapcsán az adatvédelmi felelőst az eseményről a lehető legrövidebb időn belül tájékoztatni kell, továbbá az esemény kapcsán esetlegesen kezdeményezett vizsgálatba (ellenőrzésbe) a felelőst be kell vonni.

Amennyiben személyes adat kapcsán kerül megállapításra annak jogellenes kezelése vagy feldolgozása, így különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés (a továbbiakban: adatvédelmi incidens), úgy erről az adatvédelmi felelőst haladéktalanul tájékoztatni kell. A tájékoztatásnak tartalmaznia kell az érintett személyes adatok körét, az adatvédelmi incidenssel érintettek körét és számát, az adatvédelmi incidens időpontját, körülményeit, hatásait és az elhárítására megtett intézkedéseket, valamint az adatkezelést előíró jogszabályban meghatározott egyéb adatokat.

III. FEJEZET

A SZEMÉLYES ADATOK KEZELÉSÉRE VONATKOZÓ SZABÁLYOK

A Társaságnál **személyes adat** akkor kezelhető, ha ahhoz az érintett hozzájárul vagy azt törvény, illetve törvény felhatalmazása alapján, az abban meghatározott körben - helyi önkormányzat rendelete közérdeken alapuló célból - elrendeli.

Személyes adat akkor is kezelhető, ha az érintett hozzájárulásának beszerzése lehetetlen vagy aránytalan költséggel járna, és a személyes adat kezelése

- a) az adatkezelőre vonatkozó jogi kötelezettség teljesítése céljából szükséges, vagy
- b) az adatkezelő vagy harmadik személy jogos érdekének érvényesítése céljából szükséges, és ezen érdek érvényesítése a személyes adatok védelméhez fűződő jog korlátozásával arányban áll.

Különleges adat akkor kezelhető, ha az érintett hozzájárulásának beszerzése lehetetlen vagy aránytalan költséggel járna, és a személyes adat kezelése

- a) az adatkezelőre vonatkozó jogi kötelezettség teljesítése céljából szükséges, vagy
- b) az adatkezelő vagy harmadik személy jogos érdekének érvényesítése céljából szükséges, és ezen érdek érvényesítése a személyes adatok védelméhez fűződő jog korlátozásával arányban áll.

Különleges adat akkor kezelhető továbbá, ha

- a) az adatkezeléshez az érintett írásban hozzájárul,
- b) a faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviselői szervezeti tagságra, a szexuális életre vonatkozó személyes adat esetében az törvényben kihirdetett nemzetközi szerződés végrehajtásához szükséges, vagy azt az Alaptörvényben biztosított alapvető jog érvényesítése, továbbá a nemzetbiztonság, a bűncselekmények megelőzése vagy üldözése érdekében vagy honvédelmi érdekből törvény elrendeli, vagy
- c) az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat, valamint a bűnügyi személyes adat esetében törvény közérdeken alapuló célból elrendeli.

Kötelező adatkezelés esetén az adatkezelés célját és feltételeit, a kezelendő adatok körét és megismerhetőségét, az adatkezelés időtartamát, valamint az adatkezelő személyét az adatkezelést elrendelő törvény határozza meg.

Ha a személyes adat felvételére az érintett hozzájárulásával került sor, az adatkezelő a felvett adatokat törvény eltérő rendelkezésének hiányában

- a) a rá vonatkozó jogi kötelezettség teljesítése céljából, vagy
 - b) az adatkezelő vagy harmadik személy jogos érdekének érvényesítése céljából, ha ezen érdek érvényesítése a személyes adatok védelméhez fűződő jog korlátozásával arányban áll
- további külön hozzájárulás nélkül, valamint az érintett hozzájárulásának visszavonását követően is kezelheti.

Az érintett kérelmére, kezdeményezésére indult ügyben az általa megadott személyes adatok tekintetében az érintett hozzájárulását vélelmezni kell.

Kétség esetén azt kell vélelmezni, hogy az érintett a hozzájárulását nem adta meg.

1. A személyes adat kezelésének célhoz kötöttsége

Személyes adatot kezelni csak meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében lehet. Az adatkezelésnek minden szakaszában meg kell felelnie e célnak. Csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas, csak a cél megvalósulásához szükséges mértékben és ideig.

Ha az adatkezelés célja megszűnt vagy az adatok kezelése egyébként jogellenes, az adatokat bizonylatoltan, visszaállíthatatlanul törölni/megsemmisíteni kell.

Az érintettel az adat felvétele előtt közölni kell az adatkezelés célját és azt, hogy az adatszolgáltatás önkéntes vagy kötelező. Kötelező adatszolgáltatás esetén meg kell jelölni az adatkezelést elrendelő jogszabályt, és társasági szabályozást is.

Az érintettet — egyértelműen, részletesen és dokumentáltan — **tájékoztatni kell** az adatai kezelésével kapcsolatos minden tényről, így különösen az adatkezelés céljáról és jogalapjáról, az adatkezelésre és adatfeldolgozásra jogosult személyéről, arról, ha az érintett személyes adatait az adatkezelő az Infotv. 6. § (5) bekezdése alapján kezeli, az adatkezelés időtartamáról, illetve arról, hogy kik ismerhetik meg az adatokat. A tájékoztatásnak ki kell terjednie az érintett adatkezeléssel kapcsolatos jogaira és jogorvoslati lehetőségeire is.

Az adatkezelésről való tájékoztatás megtörténik azzal is, hogy a jogszabály rendelkezik a már létező adatkezelésből továbbítással vagy összekapcsolással az adat felvételéről.

2. A személyes adat kezelésének társasági szabályai

a) Személyazonosító adatok kezelése

A munka törvénykönyvéről szóló 2012. évi I. törvény (a továbbiakban: Mt.), a foglalkoztatás elősegítéséről, a munkanélküliek ellátásáról szóló 1991. évi IV. törvény, valamint az adózás rendjéről szóló 2003. évi XCII. törvény rendelkezik a Társaság által nyilvántartható adatok köréről. Meghatározza, hogy a munkavállalótól csak olyan nyilatkozat megtétele vagy adat közlése kérhető, amely személyhez fűződő jogát nem sérti, és a munkaviszony létesítése, teljesítése vagy megszűnése szempontjából lényeges, továbbá 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, lakcím), amelyek a munkavállaló egyértelmű azonosításához szükségesek, valamint az iskolai és szakképzettséget igazoló bizonyítványok adatait. A Társaság további személyes adatokat kötelező adatkezelés keretében kezel (pl. a munkavállaló adóazo-

nosító jelét, társadalombiztosítási azonosító számát), mivel 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, leánykori név, anyja neve, születési hely és idő),
- a munkáltatónál munkaviszonyban töltött idő tartamát,
- a munkavállaló munkabéréből jogerős határozat vagy jogszabály alapján levonandó tartozást, illetve ennek jogosultját,
- a munkavállaló által a munkaviszony megszüntésének évében igénybe vett betegszabadság időtartamát,
- a munkavállaló végkielégítésben való részesülését,
- a munkáltató köteles igazolni azt is, ha a munkavállaló munkabérét a 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.
- MÁV, Volán 50%-os viteldíj-kedvezmény igénybevételének tényét.
- a Start-kártyával² kapcsolatos adatokat (amennyiben a Start-program szerinti kedvezményt vesz igénybe a Társaság).

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.

A törvényi illetve törvény felhatalmazása alapján, az abban meghatározott körben - helyi önkormányzat rendeletében foglalt előírásokban nem szereplő személyes adatok kizárólag az érintett hozzájáruló nyilatkozata alapján, illetőleg a jelen fejezetben meghatározott körülmények fennállta esetén kezelhetők, azok nyilvánosságra az Infotv-ben, a közérdekű és közérdekből nyilvános adatok közzétételére vonatkozó kötelezettségének, valamint a köztulajdonban álló gazdasági társaságok takarékosabb működéséről szóló 2009. évi CXII. törvényben (a továbbiakban: Közzétételi tv.), valamint a Közzétételi Szabályzatban foglalt esetben hozhatók, illetőleg ugyanezen szabályokban foglalt esetekben közölhetők 3. személlyel.

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

Minden személy munkabérére és egyéb járandóságára, továbbá a munkaviszony kapcsán keletkező egyéb adatok (tiszttség vagy munkakör, munkaviszonyban álló személy esetében a

² Ld. a pályakezdő fiatalok, az ötven év feletti munkanélküliek, valamint a gyermekek gondozását, illetve a családtag ápolását követően munkát keresők foglalkoztatásának elősegítéséről, továbbá az ösztöndíjas foglalkoztatásról szóló 2004. évi CXIII. törvény előírásait

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 kötelezettségének, valamint a Közzétételi tv, továbbá a Közzétételi Szabályzatban foglalt munkaköröket, illetőleg azon adatköröket, melyek közérdekből nyilvános adatnak minősülnek.

A munkabérről, munkaviszonnyal kapcsolatos egyéb személyes adatról (pl. szabadságnylvántartás, beosztás 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 személyszállítási szolgáltatás nyújtásával kapcsolatos helyen (járművek, megállóhelyek stb.) az alábbiak szerint kell eljárni (az Infotv., illetve a személyszállítási szolgáltatásokról szóló 2012. évi XLI. törvény (a továbbiakban: Sztv.) alapján):

A Társaság a vasút-, trolibusz-, autóbusz-állomáson a közforgalom számára nyitva álló helyen, a jegy- és bérletértékesítő berendezéseken, a megállóhelyen, kikötőben, valamint a személyszállító vasúti járművek, trolibuszok, az autóbuszok és a hajók, kompok belterében jogosult videómegfigyelő-rendszert alkalmazni. A videó-megfigyelő rendszer alkalmazásának a jogalapja a fentiekben meghatározott területeken lévő berendezések, a járművek, illetve a trolibusz, autóbusz rendszer eszközei, a jegy- és bérletértékesítő berendezések és a hajók, kompok, továbbá az utasok életének, személyének, testi épségének és vagyontárgyaik védelme.

Az érintettet e körben tájékoztatni kell az elektronikus biztonságtechnikai rendszer által folytatott megfigyelés, valamint a rendszer által rögzített, személyes adatokat tartalmazó kép- és hangfelvétel készítésének, tárolásának **céljáról**, az adatkezelés **jogalapjáról**, a felvétel **tárolásának helyéről**, a tárolás **időtartamáról**, a rendszert **alkalmazó (üzemeltető) személyéről**, az adatok **megismerésére jogosult személyek köréről**, továbbá a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló törvénynek az **érintettek jogaira és érvényesítésük rendjére vonatkozó rendelkezéseiről**.

A tájékoztatásnak úgy kell megvalósulnia, hogy az érintett már az adatkezelés megkezdésének a pillanatában abban a helyzetben legyen, hogy tudja: utazása/megállóban tartózkodása stb. esetén róla felvétel készül, ezért figyelemfelhívó jelzést és ismertetést kell elhelyezni

- a) a vasút-, hajó-, trolibusz- és az autóbusz-állomás és megállóhely bejáratánál,
- b) a személyszállító vasúti járműre, hajóra, trolibuszra, és az autóbuszra való felszállásra szolgáló peronoknál,
- c) a személyszállító vasúti járművön, hajón, trolibuszon és az autóbuszon, valamint
- d) a jegy- és bérletértékesítő berendezésen.

A tájékoztatásnak továbbá a vakok és gyengénlátók számára is jól érzékelhetően kell megtörténnie, így e körben Braille-írással, vagy más, arra alkalmas módon szükséges tájékoztatást nyújtani az utasoknak a kamerás megfigyelés tényéről, és arról, hogy a részletes tájékoztatás a honlapon megtalálható.

A kamerás megfigyelésre tekintettel a honlapon részletes tájékoztatást kell ezzel kapcsolatban közzétenni, és azt olyan verzióban is elérhetővé kell tenni, hogy a vakok és gyengénlátók is érzékelhessék.

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 információs önrendelkezési jogról és információszabadságról szóló 2011. évi CXII. tv. (Infotv.) 5. § (1) b) pontja alapján, a személyszállítási szolgáltatásokról szóló 2012. évi XLI. törvény (Sztv.) szerint, az utasok élete, személye, testi épsége és vagyontárgyaik védelme, valamint a járművek és az állomásokon, megállóhelyeken található berendezések védelme érdekében a BKV Zrt. elektronikus biztonságtechnikai rendszer által megfigyelést és adatrögzítést végez. Az adatkezeléssel kapcsolatos részletes tájékoztató a megállóokban erre kijelölt területen és honlapunkon olvasható.

BKV Zrt.”

A honlapon a vakok és gyengénlátók számára is érzékelhető módon az alábbi tájékoztatást kell elhelyezni:

„A BKV Zrt. az információs önrendelkezési jogról és információszabadságról szóló 2011. évi CXII. tv. (Infotv.) 5. § (1) b) pontja, illetve a személyszállítási szolgáltatásokról szóló 2012. évi XLI. törvény (Sztv.) 8. §-a alapján a vasút-, trolibusz- és az autóbusz-állomáson a közforgalom számára nyitva álló helyen, a megállóhelyen, kikötőben, valamint a személyszállító vasúti járművek, trolibuszok, az autóbuszok és a hajók, kompok belterében, a vasút-, trolibusz- és az autóbusz-állomáson, hajóállomáson és megállóhelyen elektronikus biztonságtechnikai rendszeren keresztül megfigyelést folytat.

Az elektronikus biztonságtechnikai rendszer által folytatott megfigyelés, valamint a rendszer által rögzített, személyes adatokat tartalmazó kép- és hangfelvétel készítésének, tárolásának célja fentiekben meghatározott területeken található berendezések, a személyszállító vasúti járművek, trolibusz, autóbusz, és a hajók, kompok, továbbá az utasok életének, személyének, testi épségének és vagyontárgyaik védelme.

Az adatkezelés jogalapja az Infotv. 5. §. (1) bekezdés b) pontja és az Sztv. 8. §-a.

A felvétel tárolásának helye: a műszaki adottságok függvényében a járművön, vagy központi szerveren.

A felvétel tárolásának időtartama: felhasználás hiányában a felvételt Társaságunk az elkészültét követő 16. napon törli.

A rendszert alkalmazó (üzemeltető) személye: BKV Zrt.

Az adatok megismerésére jogosult személyek köre: az Sztv. 8. § (6) bekezdése alapján bíróság vagy hatóság megkeresésére a rögzített kép-, illetve hangfelvételt a bíróságnak vagy a hatóságnak haladéktalanul meg kell küldeni. A fentiekben túl az adatokat a BKV Zrt. azon munkatársai ismerhetik meg, akiknek munkaköri kötelezettsége összefügg az adatkezelés céljának előmozdításával.

Az Infotv-nek az érintettek jogaira és érvényesítésük rendjére vonatkozó rendelkezései az alábbiak:

14. § Az érintett kérelmezheti az adatkezelőnél

a) tájékoztatását személyes adatai kezeléséről,

b) személyes adatainak helyesbítését, valamint

c) személyes adatainak - a kötelező adatkezelés kivételével - törlését vagy zárolását.

15. § (1) Az érintett kérelmére az adatkezelő tájékoztatást ad az érintett általa kezelt, illetve az általa vagy rendelkezése szerint megbízott adatfeldolgozó által feldolgozott adatairól, azok forrásáról, az adatkezelés céljáról, jogalapjáról, időtartamáról, az adatfeldolgozó nevéről, címéről és az adatkezeléssel összefüggő tevékenységéről, az adatvédelmi incidens körülményeiről, hatásairól és az elhárítására megtett intézkedésekről, továbbá - az érintett személyes adatainak továbbítása esetén - az adattovábbítás jogalapjáról és címzettjéről.

(4) Az adatkezelő köteles a kérelem benyújtásától számított legrövidebb idő alatt, legfeljebb azonban 30 napon belül, közérthető formában, az érintett erre irányuló kérelmére írásban megadni a tájékoztatást.

(5) A (4) bekezdésben foglalt tájékoztatás ingyenes, ha a tájékoztatást kérő a folyó évben azonos adatkörre vonatkozóan tájékoztatási kérelmet az adatkezelőhöz még nem nyújtott be. Egyéb esetekben költségtérítés állapítható meg. A költségtérítés mértékét a felek között létre-

jött szerződés is rögzítheti. A már megfizetett költségtérítést vissza kell téríteni, ha az adatokat jogellenesen kezelték, vagy a tájékoztatás kérése helyesbítéshez vezetett.

16. § (1) Az érintett tájékoztatását az adatkezelő csak a 9. § (1) bekezdésében, valamint a 19. §-ban meghatározott esetekben tagadhatja meg.

(2) A tájékoztatás megtagadása esetén az adatkezelő írásban közli az érintettel, hogy a felvilágosítás megtagadására e törvény mely rendelkezése alapján került sor. A felvilágosítás megtagadása esetén az adatkezelő tájékoztatja az érintettet a bírósági jogorvoslat, továbbá a Hatósághoz fordulás lehetőségéről.

17. § (1) Ha a személyes adat a valóságnak nem felel meg, és a valóságnak megfelelő személyes adat az adatkezelő rendelkezésére áll, a személyes adatot az adatkezelő helyesbíti.

(2) A személyes adatot törölni kell, ha

a) kezelése jogellenes;

b) az érintett - a 14. § c) pontjában foglaltak szerint - kéri;

c) az hiányos vagy téves - és ez az állapot jogszerűen nem orvosolható -, feltéve, hogy a törlést törvény nem zárja ki;

d) az adatkezelés célja megszűnt, vagy az adatok tárolásának törvényben meghatározott határideje lejárt;

e) azt a bíróság vagy a Hatóság elrendelte.

(3) A (2) bekezdés d) pontjában meghatározott esetben a törlési kötelezettség nem vonatkozik azon személyes adatra, amelynek adathordozóját a levéltári anyag védelmére vonatkozó jogszabály értelmében levéltári őrizetbe kell adni.

(4) Törlés helyett az adatkezelő zárolja a személyes adatot, ha az érintett ezt kéri, vagy ha a rendelkezésére álló információk alapján feltételezhető, hogy a törlés sértené az érintett jogos érdekeit. Az így zárolt személyes adat kizárólag addig kezelhető, ameddig fennáll az az adatkezelési cél, amely a személyes adat törlését kizárta.

(5) Az adatkezelő megjelöli az általa kezelt személyes adatot, ha az érintett vitatja annak helyességét vagy pontosságát, de a vitatott személyes adat helytelensége vagy pontatlansága nem állapítható meg egyértelműen.

18. § (1) A helyesbítésről, a zárolásról, a megjelölésről és a törlésről az érintettet, továbbá mindazokat értesíteni kell, akiknek korábban az adatot adatkezelés céljára továbbították. Az értesítés mellőzhető, ha ez az adatkezelés céljára való tekintettel az érintett jogos érdekét nem sérti.

(2) Ha az adatkezelő az érintett helyesbítés, zárolás vagy törlés iránti kérelmét nem teljesíti, a kérelem kézhezvételét követő 30 napon belül írásban vagy az érintett hozzájárulásával elektronikus úton közli a helyesbítés, zárolás vagy törlés iránti kérelem elutasításának ténybeli és jogi

indokait. A helyesbítés, törlés vagy zárolás iránti kérelem elutasítása esetén az adatkezelő tájékoztatja az érintettet a bírósági jogorvoslat, továbbá a Hatósághoz fordulás lehetőségéről.

19. § Az érintettnek a 14-18. §-ban meghatározott jogait törvény korlátozhatja az állam külső és belső biztonsága, így a honvédelem, a nemzetbiztonság, a bűncselekmények megelőzése vagy üldözése, a büntetés-végrehajtás biztonsága érdekében, továbbá állami vagy önkormányzati gazdasági vagy pénzügyi érdekből, az Európai Unió jelentős gazdasági vagy pénzügyi érdekből, valamint a foglalkozások gyakorlásával összefüggő fegyelmi és etikai vétségek, a munkajogi és munkavédelmi kötelezettségszegések megelőzése és feltárása céljából - beleértve minden esetben az ellenőrzést és a felügyeletet is -, továbbá az érintett vagy mások jogainak védelme érdekében.”

Azon, kamerával történő megfigyelések, melyek során rögzítés nem történik (tehát csupán élőképes megfigyelést tesz lehetővé a videómegfigyelő-rendszer), és a kamerás megfigyelés által az élőképes megfigyelésen túl többletinformációhoz nem jut a Társaság (tehát a technika segítségével nem jut több információhoz a Társaság annál, mintha az adott területet egy személy figyelné egy konkrét helyről) nem tekinthetőek adatkezelésnek (a továbbiakban: Kivételi Kör). Ennek további feltétele, hogy a kamerák ne titkos megfigyelési eszközként, hanem az ellenőrzésre jogosult jelenlétének helyettesítőjeként szolgáljanak, így minden esetben jól látható módon kell elhelyezni azokat.

A Kivételi Körbe tartozó területek vonatkozásában elegendő egy piktogramos figyelemfelhívás (pl. sárga háttéren fekete jelzéssel egy kamera látható, alatta a felirat: Kamerával megfigyelt terület, CCTV in operation), további felirat nem alkalmazandó.

A rögzített kép-, hang- vagy kép- és hangfelvételt felhasználás hiányában a rögzítéstől számított 16. napon meg kell semmisíteni vagy törölni kell. Felhasználásnak minősül, ha a rögzített kép-, illetve hangfelvétel bírósági vagy hatósági eljárásban bizonyítékként felhasználásra vagy bíróság, hatóság részére ilyen eljárás során benyújtásra kerül.

Akinek jogát vagy jogos érdekét a rögzített kép-, illetve hangfelvétel érinti, a rögzítéstől számított 15 napon belül jogának vagy jogos érdekének igazolásával kérheti, hogy a kép- illetve hangfelvételt annak kezelője ne semmisítse meg vagy ne törölje.

Ez egyben azt is jelenti, hogy azon videómegfigyelő-rendszerek esetében, ahol a kamera rögzít is, a felvételt 15 napig meg kell őrizni. Amennyiben a kamera nem rögzít, úgy természetesen ilyen kötelezettség nem terheli a Társaságot.

Bíróság vagy hatóság megkeresésére a rögzített kép-, illetve hangfelvételt a bíróságnak vagy a hatóságnak haladéktalanul meg kell küldeni. Ha a megkeresésre attól számított 72 órán belül, hogy a megsemmisítés vagy törlés mellőzését az érintett kérte, nem kerül sor, és a rögzítéstől számított 16. nap letelt, a rögzített kép- illetve hangfelvételt meg kell semmisíteni, vagy törölni kell.

Egyebekben a felvételt az a munkavállaló ismerheti meg, akiknek munkaköri kötelezettsége összefügg az adatkezelés céljának előmozdításával.

A felvétel bírósági, vagy hatósági megkeresésre történő kiadásáról, amennyiben a megkeresésre nem írásbeli formában került sor, jegyzőkönyvet kell felvenni, amiben rögzíteni kell a megkeresés feladójának pontos megjelölését (pl. Pesti Központi Kerületi Bíróság), a megkeresés ügyszámát, idejét, az ügy rövid megjelölését, a megkereséssel érintett adatok körét (pl. mely területet érintően, mely időpont vonatkozásában került kiadásra a felvétel), a kiadás pontos idejét, módját (pl. CD-n, e-mail útján, stb.), a megkeresés teljesítőjének nevét, beosztását, aláírását. A megkeresések teljesítésének részletszabályait az érintett adatokat kezelő szakterületek első számú vezetőinek kell kidolgozniuk, majd az adatvédelmi felelőssel egyeztetniük. A megkeresések teljesítésének általános követelménye azok nyomon követhető dokumentáltsága.

C.2. A munkavégzésre szolgáló helyen az alábbiak szerint kell eljárni (az Infotv.), illetve az Mt. alapján):

Az emberi élet, testi épség, személyi szabadság védelme, a veszélyes anyagok őrzése, az üzleti, fizetési, bank- és értékpapírtitok védelme, valamint vagyonvédelem érdekében alkalmazható videómegfigyelő-rendszer, 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.

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 információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Info tv.) 5. § (1) bekezdés b) pontja, valamint a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól szóló 2005. évi CXXXIII. törvény (a továbbiakban: Vtv.) 31. § (1) bekezdése alapján a BKV Zrt. vagyontárgyainak védelme érdekében elektronikus biztonságtechnikai rendszer által megfigyelést és adatrögzítést végez. Az adatok tárolása a Vtv. 31. § (2) bekezdésében meghatározott időtartamban történik. Az érintettek jogaira az Info tv. 14-19. §-ai irányadók.

BKV Zrt.”

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 jogalapjára³,
- 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,⁴
- az elektronikus megfigyelőrendszert üzemeltető (jogi vagy természetes) személy meghatározására,⁵
- a felvétel tárolásának helyére és időtartamára,⁶
- a felvételek tárolásával kapcsolatos adatbiztonsági intézkedésekre,⁷
- az adatok megismerésére jogosult személyek körére, illetőleg arra, hogy a felvételeket mely személyek, szervek részére, milyen esetben továbbíthatja,⁸
- a felvételek visszanezésére vonatkozó szabályokra, illetőleg arra, hogy a felvételeket milyen célból használhatja fel a munkáltató,⁹
- arra, hogy a munkavállalókat milyen jogok illetik meg az elektronikus megfigyelőrendszerrel összefüggésben és milyen módon tudják gyakorolni a jogaikat,¹⁰
- arra, hogy az információs önrendelkezési joguk megsértése esetén milyen jogérvényesítési eszközöket vehetnek igénybe.¹¹

A fenti kérdések vonatkozásában a videómegfigyelő-rendszert alkalmazó egyes szakterületeknek terület-specifikus szabályozást kell kialakítaniuk, az adatvédelmi felelőssel egyeztetniük, és azt a munkavállalók részére kimutathatóan oktatni kell.

A felvételek megőrzését a Vtv. – felhasználás hiányában - legfeljebb 3 munkanapnyi időtartamra teszi lehetővé. 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, repülőtéren, metrómegállóban) terrorcselekmény és közveszélyokozás megelőzése, a Büntető Törvénykönyvről szóló törvény szerint legalább je-

³ Jelen Szabályzatnak aIII.2.c) pontjának a munkavégzésre szolgáló helyre vonatkozó szabályok első bekezdése

⁴ Területileg eltérő lehet (pl.: a xxx területen található kamera elhelyezésének a célja a társasági vagyoni védelme/veszélyes anyagok védelme stb., a kamerával a munkáltató rögzítést nem, csak közvetlen megfigyelést folytat)

⁵ Területileg eltérő lehet, de jellemzően: BKV Zrt.

⁶ A Vtv. lentiekben idézett rendelkezései szerint az időtartam vonatkozásában (tehát 3 munkanap, vagy 30 nap, az adatrögzítés céljától függően)

⁷ 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.”)

⁸ Területileg eltérő lehet

⁹ A jelen Szabályzatban meghatározott alapelvek szem előtt tartásával, az adatvédelmi felelőssel egyeztetve

¹⁰ Infotv. 14-19. §-a, jelen Szabályzatban elhelyezve

¹¹ Infotv. 22. §, és 52. §

lentős 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.

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 harminc 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 egyes szakterületeknek egyedileg kell kialakítaniuk, a szabályozót, annak kiadása előtt az adatvédelmi felelőssel egyeztetni kell.

d) A forgalmi üzemeltetés során végzett hangrögzítés

A forgalomirányításban használt híradástechnikai eszközökön (például URH, FUTÁR és egyes diszpécser központok telefonjai) lebonyolított beszélgetések rögzítésre kerülnek. Ennek tényét a munkavállalókkal dokumentáltan ismertetni kell.

A hangrögzítő berendezéseken rögzített adatokat, beszélgetéseket szükség esetén a rögzítést végző szervezet vezetője, illetve annak megbízott képviselője jogosult adathordozóra kimenteni.

A beszélgetésekről készített hangfelvételt a beszélgetésben érintett munkavállalók munkáltatói jogkört gyakorló, a vasútbiztonsági szervezet munkavállalói, a Biztonsági Igazgatóság munkatársai és a BKK forgalomfelügyeleti területe jogosultak visszahallgatni.

A keletkezett adatokat a fenti személyek írásban rögzíthetik, illetve további vizsgálat céljából azokat lemásolhatják, és maguknál tarthatják, valamint a vizsgálat során bizonyítékként felhasználhatják.

A központi adatrögzítőkből kimentett, illetve visszahallgatott beszélgetésekről a rögzítés helyén naplót kell vezetni, mely tartalmazza a visszahallgatás vagy kimentés időpontját, illetve a kérelmező nevét.

Jogsabályi előírásokon alapuló adatkezelés esetén, illetőleg jelen fejezet bevezetőjében meghatározott egyes esetekben, nem kell az érintett hozzájárulását kérni.

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

e) Az adatkezelések törzskönyve

A Társaságnál létesített **személyes adatkezelésekről törzskönyvet kell vezetni, melyek tartalmát nyilvánossá kell tenni.**

A törzskönyv első példányát az annak vezetéséért felelős adatkezelést, illetve adatfeldolgozást végző szervezeti egység vezetője, második példányát az adatvédelmi felelős őrzi.

A **törzskönyv (Id. 2. Melléklet) dokumentálja** az adatkezeléssel kapcsolatos legfontosabb tényeket és körülményeket. Ezek különösen:

- az adatkezelés megnevezése,
- célja, rendeltetése,
- jogszabályi alapja (törvény, társasági szabályozás),
- kezelője (szervezeti egység, annak vezetője, illetve az adatfeldolgozást végző felelős személy neve, beosztása, irodája és telefonszáma),
- érintettek köre és száma,
- nyilvántartott adatok köre,
- adatok forrása (maga az érintett vagy más adatkezelés),
- adatfeldolgozás módszere (manuális, számítógépes, vegyes),
- az adatokon végzett gyakori adatkezelési műveletek (tárolás, módosítás, aktualizálás, válogatás, rendszerezés, stb.),
- adattovábbítás (mely szerv részére? milyen rendszerességgel?),
- adatbiztonsági intézkedések,
- adatok megőrzésének, illetve törlésének ideje.

A törzskönyv adatainak valódiságát az illetékes adatkezelő évente felülvizsgálja, az időközben történt változásokat átvezeti. Az adatkezelés megszűnése után a törzskönyvet irattári kezelésbe kell venni.

3. Adatok minőségi követelményei

A kezelt személyes adatoknak meg kell felelniük az alábbi minőségi követelményeknek:

- felvételük és kezelésük tisztességes és törvényes,
- pontosak, teljesek, időszerűek,
- tárolásuk módja alkalmas arra, hogy az érintettet csak a tárolás céljához szükséges ideig lehessen azonosítani.

Korlátozás nélkül használható, általános és egységes személyazonosító jel alkalmazása tilos.¹²
A tárolás módjára vonatkozó technikai megoldásokat és feltételeket az Informatikai Biztonsági Szabályzat tartalmazza.

4. 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. közérdekből nyilvános adatokra vonatkozó rendelkezései, valamint a Közzétételi Szabályzat tartalmazza. 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) Adatkezelések összekapcsolása

A Társaságnál folyó, különböző célra irányuló adatkezelések csak törvényes cél érdekében, indokolt esetben, ideiglenesen kapcsolhatók össze.

Az **adatkezelések összekapcsolásával kapcsolatos tényeket jegyzőkönyvbe (ld. 3. Melléklet)** kell foglalni:

A jegyzőkönyv első példányát az adatkezelés helyén kell őrizni, második példányát az adatvédelmi felelőshöz kell továbbítani. A jegyzőkönyvet 10 évig kell megőrizni.

c) Belföldre irányuló adattovábbítások

A Társaságon kívüli szervtől vagy magánszemélytől érkező, személyes adat közlésére irányuló megkeresés csak akkor teljesíthető, ha az érintett erre írásban felhatalmazza a Társaságot, vagy azt törvény illetve törvény felhatalmazása alapján, az abban meghatározott körben - helyi önkormányzat rendelete közérdeken alapuló célból elrendeli. Az érintett előzetesen is adhat ilyen tartalmú felhatalmazást, amely szólhat 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 adat szolgáltatás csak az adatkezelést végző szervezeti egység munkáltatói jogkört gyakorló vezetőjének jóváhagyásával teljesíthető.

¹² Nem sorolható ide a Társaságnál alkalmazott, a munkavállalók egyedi azonosítására szolgáló törzsszám.

A nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény 42. §-a szerint az az adatkezelő szerv, amely a nemzetbiztonsági szolgálatok részére az általa kezelt nyilvántartásokból adat-szolgáltatást 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 tájékoztat-hat.

A megkeresés alapján teljesített **adatszolgáltatással kapcsolatos tényeket, körülményeket jegyzőkönyv (ld. 4. Melléklet)** felvételével dokumentálni kell (kivételt képeznek a hatósági, a Társaság munkavállalóinak munkaviszonyával kapcsolatos megkeresések, pl. NAV-tól, bíróság-tól, nemzetbiztonsági szolgálatoktól érkező megkeresések).

A megkeresésről szóló jegyzőkönyv első példányát az adatkezelés helyén kell, 10 évig megőriz-ni.

d) Külföldre irányuló adattovábbítások

Olyan adatkezelés esetén, amelynél számolni kell harmadik országba irányuló — az adathordo-zótól vagy az átvitel módjától függetlenül — adattovábbítással, az érintettek figyelmét erre a körülményre már az adatok felvétele előtt fel kell hívni. A személyes adat csak akkor továbbít-ható, ha ahhoz az érintett írásban hozzájárul, vagy azt az Infotv, vagy egyéb törvény lehetővé teszi, vagy arról nemzetközi szerződés rendelkezik, feltéve, hogy a harmadik ország joga — az Európai Unió által meghatározott — megfelelő védelmet biztosít az átadott adatok kezelése során.

A **külföldre irányuló adatszolgáltatással kapcsolatos tényeket, körülményeket jegyzőkönyv (ld. 5. Melléklet)** felvételével dokumentálni kell.

A külföldre irányuló adattovábbításról szóló jegyzőkönyv első példányát az adatkezelés helyén kell őrizni, második példányát az adatvédelmi felelőshöz kell továbbítani. A jegyzőkönyvet 10 évig kell megőrizni.

5. Érintettek jogai és érvényesítésük

a) Tájékoztatásra, illetve betekintésre irányuló kérelem

Az érintett tájékoztatást, illetve betekintést kérhet személyes adatai kezeléséről, valamint kér-heti személyes adatainak helyesbítését, illetve — a jogszabályban elrendelt adatkezelések kivé-telével — törlését vagy zárolását. A betekintést úgy kell biztosítani, hogy ez alatt az érintett más személy adatait ne ismerhesse meg.

Az érintett kérelmére az adatkezelő tájékoztatást ad az érintett általa kezelt, illetve az általa vagy rendelkezése szerint megbízott adatfeldolgozó által feldolgozott adatairól, azok forrásáról, az adatkezelés céljáról, jogalapjáról, időtartamáról, az adatfeldolgozó nevéről, címéről és az

adatkezeléssel összefüggő tevékenységéről, az adatvédelmi incidens körülményeiről, hatásairól és az elhárítására megtett intézkedésekről, továbbá - az érintett személyes adatainak továbbítása esetén - az adattovábbítás jogalapjáról és címzettjéről.

A Társaság, a belső adatvédelmi felelős útján, az adatvédelmi incidenssel kapcsolatos intézkedések ellenőrzése, valamint az érintett tájékoztatása céljából nyilvántartást vezet, amely tartalmazza az érintett személyes adatok körét, az adatvédelmi incidenssel érintettek körét és számát, az adatvédelmi incidens időpontját, körülményeit, hatásait és az elhárítására megtett intézkedéseket, valamint az adatkezelést előíró jogszabályban meghatározott egyéb adatokat.

A fenti nyilvántartás időtartamát, az adatkezelést szabályozó jogszabály korlátozhatja. A korlátozás időtartama személyes adatok esetében 5 évnél, különleges adatok esetében pedig 20 évnél rövidebb nem lehet.

Az érintett tájékoztatást, illetve betekintést kérhet a Társaságnál vezetett adatkezelési törzskönyv tartalmába is.

A tájékoztatást a kérelemben foglaltakra az illetékes adatkezelő (az adatkezelést végző szervezeti egység vezetője) adja meg. A tájékoztatást a benyújtástól számított legrövidebb idő alatt, legfeljebb azonban 30 napon belül írásban, közérthető formában kell megadni.

b) Tájékoztatásra, illetve betekintésre irányuló kérelem megtagadása

A tájékoztatás, illetve betekintés az Infotv. 9. §, és 19. §-ban foglaltak alapján kizárólag akkor **tagadható meg**, ha azt

- törvény korlátozza az állam külső és belső biztonsága, így a honvédelem, a nemzetbiztonság, a bűnmegelőzés vagy a bűnüldözés, a büntetés-végrehajtás biztonsága érdekében,
- továbbá állami vagy önkormányzati gazdasági vagy pénzügyi érdekből,
- illetve az Európai Unió jelentős gazdasági vagy pénzügyi érdekből,
- valamint a foglalkozások gyakorlásával összefüggő fegyelmi és etikai vétségek, a munkajogi és munkavédelmi kötelezettségszegések megelőzése és feltárása céljából — beleértve minden esetben az ellenőrzést és a felügyeletet is —,
- továbbá az érintett vagy mások jogainak védelme érdekében.

A tájékoztatás, illetve betekintés korlátozható, ha törvény, nemzetközi szerződés vagy az Európai Unió kötelező jogi aktusának rendelkezése alapján az adatkezelő személyes adatot akként vesz át, hogy az adattovábbító adatkezelő az adattovábbítással egyidejűleg jelzi a személyes adat

- a) kezelésének lehetséges célját,
- b) kezelésének lehetséges időtartamát,
- c) továbbításának lehetséges címzettjeit,
- d) érintettje e törvényben biztosított jogainak korlátozását, vagy
- e) kezelésének egyéb korlátozását

(a továbbiakban: együtt: adatkezelési korlátozás).

Ez esetben a személyes adatokat átvevő adatkezelő a személyes adatot az adatkezelési korlátozásnak megfelelő terjedelemben és módon kezeli, az érintett jogait az adatkezelési korlátozásnak megfelelően biztosítja.

Elutasítás esetén az adatkezelő tájékoztatja az érintettet a felvilágosítás megtagadásának indokáról, illetve a bírósági jogorvoslat, továbbá a Nemzeti Adatvédelmi és Információszabadság Hatósághoz (a továbbiakban: Hatóság) fordulás lehetőségéről. Ezzel egyidejűleg a megtagadásról írásban tájékoztatja az adatvédelmi felelőst.

Az adatvédelmi felelős minden év január 31-ig értesíti a Hatóságot az elutasított kérelmekről.

c) Személyes adat helyesbítése, törlése, megjelölése, illetve zárolása

A személyes adat helyesbítését, törlését, megjelölését, illetve zárolását a helyesbítés, törlés, megjelölés, zárolás tárgya szerinti szakterület végzi el személyes észlelés alapján, kérelemre vagy az adatvédelmi felelős felhívására. A helyesbítésről, törlésről és zárolásról az érintettet, továbbá mindazokat értesíteni kell, akiknek korábban az adatot adatkezelés céljára továbbították. Az értesítés mellőzhető, ha ez az adatkezelés céljára való tekintettel az érintett jogos érdekeit nem sérti. A helyesbítést, illetve törlést 3 munkanapon belül el kell végezni.

Ha az adatkezelés célja megszűnt, vagy az adatok tárolásának törvényben előírt határideje lejárt, úgy a törlési kötelezettség — a jogellenes adatkezelés kivételével — nem vonatkozik azon személyes adatokra, amelyeknek adathordozóját a levéltári anyag védelmére vonatkozó jogszabály értelmében levéltári őrizetbe kell adni.

Törlés helyett az adatkezelő **zárolja** a személyes adatot, ha az érintett ezt kéri, vagy ha a rendelkezésére álló információk alapján feltételezhető, hogy a törlés sértené az érintett jogos érdekeit. Az így zárolt személyes adat kizárólag addig kezelhető, ameddig fennáll az az adatkezelési cél, amely a személyes adat törlését kizárta.

Az adatkezelő **megjelöli** az általa kezelt személyes adatot, ha az érintett vitatja annak helyességét vagy pontosságát, de a vitatott személyes adat helytelensége vagy pontatlansága nem állapítható meg egyértelműen.

d) Tiltakozás a személyes adat kezelése ellen

Az Infotv. 21. §-ban felsorolt feltételek alapján, **az érintett tiltakozhat** személyes adatának kezelése ellen, ha

- a személyes adatok kezelése vagy továbbítása kizárólag az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez vagy az adatkezelő, adatátvevő vagy harmadik személy jogos érdekének érvényesítéséhez szükséges, kivéve kötelező adatkezelés esetén;
- a személyes adat felhasználása vagy továbbítása közvetlen üzletszerzés, közvélemény-kutatás vagy tudományos kutatás céljára történik;
- a tiltakozás jogának gyakorlását egyébként törvény lehetővé teszi.

Az adatkezelő — az adatkezelés egyidejű felfüggesztésével — a tiltakozást köteles a kérelem benyújtásától számított legrövidebb időn belül, de legfeljebb 15 nap alatt megvizsgálni, és annak eredményéről a kérelmezőt írásban tájékoztatni. Amennyiben a tiltakozás indokolt, az adatkezelő köteles az adatkezelést — beleértve a további adatfelvételt és adattovábbítást is — megszüntetni és az adatokat zárolni, valamint a tiltakozásról, illetőleg az annak alapján tett intézkedésekről értesíteni mindazokat, akik részére a tiltakozással érintett személyes adatot korábban továbbította, és akik kötelesek intézkedni a tiltakozási jog érvényesítése érdekében. Az adatvédelemmel összefüggő bejelentések, tiltakozások kivizsgálásához az adatvédelmi felelős megkeresésre segítséget nyújt, iratanyag bekérésével vagy a helyszínen.

A bejelentést, tiltakozást beérkezésétől számított 3 munkanapon belül a szakterület döntése alapján továbbítani kell az adatvédelmi felelőshöz — kivéve azt az esetet, amikor azt eredetileg az adatvédelmi felelőshöz nyújtották be.

Az adatvédelmi felelős a hozzá beérkezett bejelentést 30 napon belül, a tiltakozást a legrövidebb időn belül, de legfeljebb — az eredeti benyújtástól számított — 15 napon belül vizsgálja ki. A vizsgálat eredményéről értesíti az érintettet és a bejelentés, tiltakozás helye szerinti szervezeti egységet — valamint ha ettől különbözik, az adatkezelőt is.

Adatkezeléssel kapcsolatos jogainak megsértése esetén az érintett az illetékes adatkezelő szervezeti egység vezetőjéhez, az adatvédelmi felelőshöz vagy a Hatósághoz fordulhat; ezen bejelentések miatt senkit sem érhet hátrány.

Az adatkezelést végző szervezeti egység vezetője és az érintett közötti vitában a jogi igazgató és a belső adatvédelmi felelős dönt. Az Infotv. 21. §-ának értelmében a döntés ellen az érintett bírósághoz fordulhat, ahol az ügyben soron kívül járnak el.

6. Adatfeldolgozó igénybevételeinek szabályai

Az adatkezelő az adatok feldolgozásával kapcsolatos műveletek elvégzésére adatfeldolgozót vehet igénybe. Az adatfeldolgozónak a személyes adatok feldolgozásával kapcsolatos jogait és kötelezettségeit az Infotv., valamint az adatkezelésre vonatkozó külön törvények keretei között az adatkezelő határozza meg. **Az adatfeldolgozásra vonatkozó megbízási szerződést írásba kell foglalni.**

a) Az adatkezelő felelőssége

- Az adatkezelési műveletekre vonatkozó utasítások jogszerűségéért az adatkezelő felel.
- A Társaság külső adatfeldolgozót is igénybe vehet.
- Adatfeldolgozásra nem adható megbízási olyan vállalkozásnak, amely a feldolgozandó személyes adatokat felhasználó üzleti tevékenységében érdekelt.
- A Társaság által igénybe vett adatfeldolgozó esetében szerződésben meghatározott szigorú szabályok szerint kell eljárni, melyek betartásáról rendszeres ellenőrzéssel kell meggyőződni (az ellenőrzést a Társaság részéről a szerződést aláíró vezetők végzik).

b) Az adatfeldolgozó felelőssége

- Az adatfeldolgozó tevékenységi körén belül, illetőleg az adatkezelő által meghatározott keretek között felelős a személyes adatok feldolgozásáért, megváltoztatásáért, törléséért, továbbításáért és nyilvánosságra hozataláért.
- Az adatfeldolgozó tevékenységének ellátása során más adatfeldolgozót az adatkezelő rendelkezése szerint vehet igénybe.
- Az adatfeldolgozó az adatkezelést érintő érdemi döntést nem hozhat, a tudomására jutott személyes adatokat kizárólag az adatkezelő rendelkezései szerint dolgozhatja fel, saját céljára adatfeldolgozást nem végezhet, továbbá a személyes adatokat az adatkezelő rendelkezései szerint köteles tárolni és megőrizni.

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, kivéve, ha az adatot törvény alapján az arra jogosult szerv minősített adattá nyilvánította, 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 a vezérigazgató e határidőn belül is engedélyezheti.

A közérdekű adatok megismerésével és nyilvánosságával összefüggésben az üzleti titok megismerésére a Ptk.-ban foglaltak a jelen Szabályzatban foglalt eltérésekkel az irányadók.

A közérdekű adat megismerése

1. A közérdekű adatok megismerésére irányuló — szóban, írásban vagy elektronikus úton érkező — kérelemnek a szakigazgatóság 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.

2. 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 (jelen Szabályzat hatályba lépésekor a 10/VU/2015. sz. utasításban; (a továbbiakban: Utasítás)) meghatározott esetekben és összegek alapul vételével költségtérítést állapíthat meg, amelynek összegéről az érintett szakterületnek 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 érintett szakterület 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 munkaerőforrás 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.

3. 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 felelőst.

Az adatvédelmi felelős évente, minden év január 31. napjáig értesíti a Hatóságot 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 — a szakterület vezetőjének az adatvédelmi felelős tájékoztatásával egyidejűleg a Jogi és Humánpolitikai Igazgatóság állásfoglalását kell kérnie (ettől függetlenül a kérelmező — és vele egyidejűleg az adatvédelmi felelős — írásos értesítése 8 napon belül kell, hogy megtörténjen, így a megkereséseket ennek figyelembevételével kell megtenni).

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

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

V. FEJEZET

AZ ADATVÉDELEM ÉS ADATBIZTONSÁG TECHNIKAI HÁTTERÉNEK EGYES KÉRDÉSEI, IRATMINŐSÍTÉSI ALAPELVEK

Az Infotv. rendelkezései szerint az adatkezelő, illetőleg tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek a törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.

Az adatokat védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés ellen. A személyes adatok technikai védelmének biztosítása érdekében külön védelmi intézkedéseket kell tennie az adatkezelőnek, az adatfeldolgozónak, illetőleg a távközlési vagy informatikai eszköz üzemeltetőjének, ha a személyes adatok továbbítása hálózaton vagy egyéb informatikai eszköz útján történik.

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

1. Az infrastruktúrához kapcsolódó védelmi intézkedések

Irattáraknál, zárt helyiségbe (pl. gépterem) történő informatikai eszközök telepítésénél, biztosítani kell a tűzvédelmet, 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) Informatikai rendszerek osztályozási irányelvei

Az informatikai rendszereket két szempont alapján kell osztályozni:

- a rendszerben kezelt információ bizalmassága, illetve
- a rendszerrel megvalósított információfeldolgozás, adatszolgáltatás rendelkezésre állása szempontjából.

A rendszerrel kezelt információ bizalmassága szerinti osztályozás

A bizalmasság alapján történő osztályozás során meg kell vizsgálni, hogy a bizalmasság megsértése milyen következményekkel járhat. A következő fajtaikat célszerű megkülönböztetni:

- dologi kár,
- gazdasági károk,
- károk a munkahelyi és a fogyasztói bizalom területén,
- károk a személyi biztonság területén.

Meg kell vizsgálni továbbá a törvényi előírásokból adódó kötelezettségek megtartásának feltételeit. Ezek alapján az informatikai rendszereket bizalmasságuk szerint három biztonsági szintre (osztályba) sorolhatjuk be.

A rendszer besorolása	Kritériumok	Példa
Szigorúan bizalmas rendszerek	Azon informatikai rendszerek, melyek hozzáférés korlátozási sérülése: – jelentős, közvetlen anyagi kárt okoz, – hosszútávra rontja a versenypozíciót, – közvetlen súlyosan elmarasztaló jogi következményekkel jár, – a menedzsment bizalomvesztését vagy leváltását okozhatja, – emberéletpont veszélyeztető szabotázs vagy terrorcselekmények megtervezéséhez, kivitelezéséhez közvetlenül felhasználható kulcs-elem. A jelen Szabályzat 2. pontja alapján minősített – megemelt, – fokozott vagy – kiemelt biztonsági szintű adatokat kezelő informatikai rendszerek.	jelszavak, belépési kódok, biometrikus adatok, elektronikus aláírások, titkosító kulcsok az információbiztonsági dokumentáció részei stratégiai fejlesztési vagy beruházási tervek, a kapcsolódó döntés előkészítő anyagok, és az ezeket megalapozó kimutatások adatai szabadalmak személyi döntések dokumentumai igazgatósági ülések prímerek jegyzőkönyvei személyi biztonsági, élet- és balesetvédelmi rendszerek dokumentációi, üzemviteli szabályzatai

A rendszer besorolása	Kritériumok	Példa
Bizalmas rendszerek	Azon informatikai rendszerek, melyek hozzáférés korlátozási sérülése: – kis összegű anyagi kárt okoz, – a versenyelőny pillanatnyi elvesztésével jár, – peren kívüli megegyezés lehetséges, – részleges bizalomvesztés, ami a szervezeten belül marad, – emberéletet nem veszélyeztető, de az üzletmenet folytonosságát veszélyeztető szabotázs tervezésére, kivitelezésére ad lehetőséget. A jelen Szabályzat 2. pontja alapján – alap biztonsági szintű adatokat kezelő informatikai rendszerek.	az Információbiztonsági dokumentáció részei szerzői jogú dokumentumok, szoftverek, licencek az Infotv.-ben meghatározottak alapján a személyes adatok
Nyilvános rendszerek	Az adatok nyilvánossá tétele a Társaság érdeke vagy törvényi kötelezettsége. Az adat mások számára nem értékes. Nem esik az adatvédelem körébe.	bármilyen, ami nem tartozik az előző két kategóriába

Az információ rendelkezésre állása alapján történő osztályozás

A rendelkezésre állás alapján történő osztályozás során meg kell vizsgálni, hogy az információ a Társaság üzletileg kritikus folyamatainak működtetése szempontjából mennyire fontos.

Üzletileg kritikus rendszernek minősítjük mindazon informatikai rendszereket amelyek:

- az üzletileg kritikus folyamatok működtetéséhez folyamatosan, vagy rendszeresen ismétlődően rendelkezésre kell álljanak,

- az elvesztésük vagy sérülésük esetén pótlásuk az adott üzleti folyamat rendelkezésre állása szempontjából jelentős késedelemmel, túlmunkával vagy túlzott anyagi ráfordítással járna, illetve
- szigorúan bizalmas besorolással rendelkeznek.

A fenti tulajdonságokkal nem rendelkező informatikai rendszereket és eszközöket üzletileg nem kritikus rendszernek minősítjük.

c) Az információs vagyonelemek osztályozása

- A vagyonleltárban meghatározott tulajdonosok feladata az osztályozás eredményét a vagyonleltárban is fel kell tüntetni.
- Az információhordozók osztályozása az éppen rajtuk tárolt információval azonos vagy annál magasabb lehet, ennek aktualizálása az információhordozó tulajdonosának a feladata.
- Az információ-feldolgozó rendszerek osztályozása a rajtuk feldolgozott (továbbított) legmagasabb besorolású információ besorolásával azonos, vagy annál magasabb kell legyen.

2. Eseti biztonsági intézkedések

Eseti biztonsági intézkedés akkor szükséges, amikor valamely biztonsági szint nem felel meg az adott feladat biztonsági követelményeinek.

Az adott üzemeltető szervezeti egységnél eseti biztonsági intézkedés szükséges, amennyiben magasabb biztonsági fokozatot követelő munkavégzés igénye merül fel.

Amennyiben az adott biztonsági fokozatot meghaladó munkavégzés rendszeressé válik, a biztonsági fokozat megváltoztatására — az üzemeltető kezdeményezésére — az informatikai főosztályvezető tesz javaslatot.

3. 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 vállalti mobil eszközökön elhelyezett információk visszaállíthatatlan (végleges) törléséről is az eszközök leadása esetén. Ennek részleteit az Informatikai Biztonsági Szabályzat írja elő.

4. A szoftverekhez kapcsolódó védelmi intézkedések

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

Külső szakértők számára — az IT-Szolgáltatók 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.

5. Katasztrófhelyzetek kezelése

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

6. 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.

7. Az információ kezelésével kapcsolatos intézkedések

A bizalmas és szigorúan bizalmas osztályozású információ-feldolgozó rendszerekkel történő munkavégzés során az alábbiakat kell betartani.

- Azokra a munkafolyamatokra, ahol bizalmas vagy szigorúan bizalmas osztályozású 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 bizalmas és szigorúan bizalmas elektronikus dokumentumokba (pl. Word, Excel dokumentum) külső dokumentumot csatolással beilleszteni tilos, mert a csatolt állomány esetleges törlésével a bizalmas dokumentum információtartalma sérülhet.
- Bizalmas és szigorúan bizalmas 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.
- Minden bizalmas vagy szigorúan bizalmas dokumentum nyomtatását követően a nyomtatóból azt azonnal ki kell venni. A hálózati nyomtatóból a nyomtatot 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 engedélyezőknek milyen típusú engedélyt szabad kiadnia. Az engedélyeket formalizálni kell.

- A munkafolyamatok megszakítása idejére (pl. ebédszünet) a bizalmas és szigorúan bizalmas információkat tartalmazó adathordozókat, kinyomtatott dokumentumokat, a rosszindulatú hozzáféréstől és a sérülésektől védetten kell tárolni, zárt iratszekrényben (a szigorúan bizalmas adathordozókat páncélszekrényben (kazettában)).

8. Iratminősítési alapelvek

A Társaságon belüli nemzeti minősített adatokat tartalmazó iratok **négy kategóriába** sorolhatók, ezek megjelölése: „Szigorúan titkos!”, „Titkos!”, „Bizalmas!”, „Korlátozott terjesztésű!”).

A Társaságon belüli további megjelölések:

- üzleti titok („Üzleti titok” megjelöléssel; lsd. II. fejezet 1.e) pont, minősítésre jogosultak: vezérigazgató-helyettesek, igazgatók, irodavezetők, főosztályvezetők),
- nem nyilvános irat („Nem nyilvános” megjelöléssel), valamint
- nyílt irat (megjelölés nélkül).

„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 elnök-vezérigazgató, a vezérigazgató-helyettesek, igazgatók, a belső ellenőrzési főosztályvezető és a társasági kapcsolatok irodavezető.

„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, illetve az informatikai rendszerek használata során betartandó biztonsági előírásokat pedig az Informatikai Biztonsági Szabályzat tartalmazza részletesen.

VI. FEJEZET

AZ ADATVÉDELMI FELELŐS FELADATAI, JOGAI, KÖTELEZETTSÉGEI ÉS FELELŐSSÉGE

1. Az adatvédelmi felelős Infotv.-ben meghatározott feladatai

- a) közreműködik, illetve segítséget nyújt az adatkezeléssel összefüggő döntések meghozatalában, valamint az érintettek jogainak biztosításában;
- b) ellenőrzi az Infotv. és az adatkezelésre vonatkozó más jogszabályok, valamint a belső adatvédelmi és adatbiztonsági szabályzatok rendelkezéseinek és az adatbiztonsági követelményeknek a megtartását;
- c) kivizsgálja a hozzá érkezett bejelentéseket, jogosulatlan adatkezelés észlelése esetén annak megszüntetésére hívja fel az adatkezelőt vagy az adatfeldolgozót;
- d) elkészíti a belső adatvédelmi és adatbiztonsági szabályzatot;
- e) vezeti a belső adatvédelmi nyilvántartást;
- f) gondoskodik az adatvédelmi ismeretek oktatásáról.

2. Az adatvédelmi felelős további, társasági szempontból lényeges feladatai

- A belső ellenőrzési főosztályvezető és a biztonsági igazgató tájékoztatása mellett, a jogi és humánpolitikai igazgató által jóváhagyott éves adatvédelmi ellenőrzési tervet készít, illetve jelentést annak végrehajtásáról és eredményéről.
- 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.
- A Társaság munkavállalói vonatkozásában segítséget nyújt az adatvédelmi és adatbiztonsági tevékenység végzéséhez.
- Elkészíti és aktualizálja a Társaság egészére vonatkozó adatvédelmi és adatbiztonsági rendszabályokat.
- A szakterület vezetőjének megkeresésére az adatvédelmet és adatbiztonságot érintő szakmai kérdésekben javaslatot tesz, illetve segítséget nyújt.
- A szakterület vezetőjének kérésére véleményezi az adatvédelmi biztosnak címzett, megküldés előtt álló hivatalos megkereséseket és egyéb dokumentumokat.

3. Az adatvédelmi felelős jogai

- Az ellenőrzött területre, illetve bármely helyiségbe, létesítménybe, ahol adatkezelés folyik, beléphet.¹³
- 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 vétele esetén az eredeti bizonylatot is lefoglalhatja, és magával viheti.¹⁴
- 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.
- Írásbeli nyilatkozatok, papíralapú vagy elektronikus levél formájában történt megkeresésekre az adatvédelmi felelős válaszadási határidőt jelölhet ki.
- Az ellenőrzéssel kapcsolatban a bizonylatok valódiságának ellenőrzése vagy az adatok kiegészítése céljából az adatvédelmi felelős külső szerveket is megkereshet.¹⁵
- Az adatvédelmi felelős részére teljes betekintési (olvasási) jog a Társaságnál használt SAP rendszer HR moduljába céllenőrzéshez adható, az SAP HR modul felelős előzetes tájékoztatását követően..
- Az adatvédelmi felelős az adatvédelmi ellenőrzések kapcsán felmerülő, a Társaságnál használt informatikai rendszerekhez szükséges (ideiglenes) jogosultság-igények soron kívüli, rövidebb időn belüli beállítását kérheti az Informatikai Főosztálytól.
- Tájékoztatást kérhet bármely, a Társaságnál használt informatikai rendszerekben történő jogosultság-módosításokkal kapcsolatosan.

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

¹³ Az erre vonatkozó külön szabályok figyelembevételével.

¹⁴ Másolat visszahagyása mellett.

¹⁵ Külön vezérgazdái engedéllyel.

4. Az adatvédelmi felelős kötelességei

Az adatvédelmi felelős köteles:

- a Szabályzat aktualizálását az előírtaknak megfelelően kezdeményezni,
- a Hatóságnak 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 egység vezetőjével, valamint az érdekeltekkel ismertetni,
- az ellenőrzés lezárásakor az adatvédelmi ellenőrzési jelentés egy példányát az ellenőrzött szervezeti egység munkáltatói jogkört gyakorló vezetőjének átadni,
- az adatvédelmi ellenőrzés megállapításaira adott jelentéseket értékelni,
- az adatvédelmi ellenőrzéssel kapcsolatos kötelességekre az ellenőrzött munkavállalók figyelmét felhívni és jogaikról tájékoztatni,
- az eljárása során tudomására jutott minősített adatot megőrizni,
- továbbá az ellenőrzések során, illetve az ahhoz nem kapcsolódó, de tudomására jutott bizalmas információkat (pl. személyes adatok) megőrizni.

5. Az adatvédelmi felelős felelőssége

Az adatvédelmi felelős 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 előírászerű bizonyításáért.

VII. FEJEZET

AZ ADATVÉDELMI ELLENŐRZÉSBEN ÉRINTETTEK JOGAI, KÖTELEZETTSÉGEI ÉS FELELŐSSÉGE

Az adatvédelmi ellenőrzés alapvetően az Éves adatvédelmi ellenőrzési terven alapul, melyet az adatvédelmi felelős javaslata alapján a belső ellenőrzési főosztályvezető, valamint a biztonsági igazgató tájékoztatása mellett a jogi és humánpolitikai igazgató hagy jóvá. Ezen kívül alapulhat elnök-vezérigazgatói, belső ellenőrzési főosztályvezetői, jogi és humánpolitikai- és biztonsági igazgatói, valamint az adatvédelmi felelős 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 felelős által feltett kérdésekre a valós tényeknek megfelelően szóban vagy írásban nyilatkozni,
- az adatvédelmi felelős megkeresésében kijelölt válaszadási határidőn belül válaszát a felelőshöz eljuttatni,
- elősegíteni a tapasztalható hibák, mulasztások teljes körű feltárását, illetve keletkezésük valódi okainak megismerését,
- az adatvédelmi felelős 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 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:

- meggyőződhetnek 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 felelős figyelmét felhívják,
- személyiségi jogukat sértő kérdésekben a válaszadást megtagadják (a személyiségi jog sérülésével kapcsolatos vita esetén a jogi és humánpolitikai igazgató állásfoglalását kell kérni).

3. Az adatvédelmi ellenőrzést elrendelő vezető kötelessége

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

- bűncselekmény gyanúja esetén további bizonyítékokat beszerezni, konzultálni az illetékes (nem érintett) vezetőkkal, 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 elrendelő vezető kezdeményezése alapján a munkáltatói jogkör gyakorlója köteles a fegyelmi eljárást lefolytatni, és annak eredményéről az ellenőrzést végző szervezetet 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 elnök-vezérigazgató által elrendelt eseti ellenőrzés esetén a jelen pontban meghatározott intézkedéseket a belső ellenőrzési főosztályvezető végzi el.

VIII. FEJEZET

AZ ADATVÉDELMI NYILVÁNTARTÁS

1. Bejelentkezés a nyilvántartásba

Az adatkezelésekkel kapcsolatosan az érintett szakterület megkeresésére, a Társaság képviselőiben az adatkezelő köteles a személyes adatok kezelésének megkezdése előtt a Hatóságnak nyilvántartásba vétel végett bejelenteni

- az adatkezelés célját;
- az adatkezelés jogalapját;
- az érintettek körét;
- az érintettek vonatkozó adatok leírását;
- az adatok forrását;
- az adatok kezelésének időtartamát;
- a továbbított adatok fajtáját, címzettjét és a továbbítás jogalapját, ideértve a harmadik országokba irányuló adattovábbításokat is;
- az adatkezelő, valamint az adatfeldolgozó nevét és címét (székhelyét), a tényleges adatkezelés, illetve az adatfeldolgozás helyét és az adatfeldolgozónak az adatkezeléssel összefüggő tevékenységét;
- az alkalmazott adatfeldolgozási technológia jellegét;
- a belső adatvédelmi felelős nevét és elérhetőségi adatait.

A bejelentés elkészítéséhez az adatvédelmi felelős kérésre segítséget nyújt, fent felsorolt adatok megváltozását az adatvédelmi felelős 8 napon belül köteles bejelenteni a Hatóságnak, és intézkedni a nyilvántartás megfelelő módosításáról. A nyilvántartásba vételről szóló határozat az adatvédelmi felelőshöz érkezik, azt haladéktalanul továbbítja az illetékes szakterület felé.

Az adatkezelés nyilvántartásba vételekor a Hatóságtól kapott nyilvántartási számot az adatok minden továbbításnál, nyilvánosságra hozásánál és az érintettnek való kiadásakor fel kell tüntetni.

Az adatvédelmi nyilvántartási számot — annak rendelkezésre állását követően — az adatvédelmi felelőssel ismertetni kell. A nyilvántartási szám megismerését követően a szervezeti egységek adatkezelési gyakorlatuk során az érintettel is ismertetik a nyilvántartási számot.

Nem kell bejelenteni az adatvédelmi nyilvántartásba azt az adatkezelést, amely

- az adatkezelővel munkaviszonyban, tagsági, tanulói vagy tanulószerveződéses jogviszonyban, ügyfélkapcsolatban álló személyek adatait tartalmazza (azaz a Társaság munkavállalóiról vezetett személyügyi nyilvántartásokat);
- az érintett anyagi és egyéb szociális támogatása céljából nyilvántartott személyes adatokra vonatkozik

- a hatósági, az ügyészségi és a bírósági eljárás által érintett személyeknek az eljárás lefolytatásával kapcsolatos személyes adatait tartalmazza;
- a hivatalos statisztika célját szolgáló személyes adatokat tartalmaz, feltéve, hogy — törvényben meghatározottak szerint — az adatok személlyel való kapcsolatának megállapítását véglegesen lehetetlenné teszik;
- a tudományos kutatás céljait szolgálja, ha az adatokat nem hozzák nyilvánosságra;
- az adatkezelőtől levéltári kezelésbe került át.

2. Új adatállomány feldolgozása

A Társaság működése során keletkezhetnek olyan tetszőleges szempont szerint rendszerezett, eddig nem létező, személyes adat(ok)ból álló adatállományok, adatbázisok, melyeket a Társaságnak kezelnie (feldolgoznia, továbbítania, stb.) szükséges.

Új adatállomány feldolgozását vagy új adatfeldolgozási technológia alkalmazását megelőzően a Hatóság előzetes ellenőrzést végezhet munkaügyi és bűnügyi adatállományok kezelését végző adatkezelőknél.

Az adatkezelőnek a Társaság új adatállomány feldolgozására vagy az új adatfeldolgozási technológia alkalmazására irányuló szándékát a tevékenység megkezdése előtt 30 nappal be kell jelenteni a Hatóságnak. A bejelentéshez az adatvédelmi felelős segítséget nyújt.

(A Hatóság az előzetes ellenőrzésre vonatkozó igényét a bejelentéstől számított 8 napon belül jelzi az adatkezelőnek, és az ellenőrzést 40 napon belül elvégzi.)

Ennek biztosítékeként **a szakterület a tevékenység megkezdése előtt legalább 55 nappal kérésre meg az adatvédelmi felelőst írásban**, és kérheti a felelős álláspontját.

A Társaság az adatfeldolgozást csak a Hatóság előzetes ellenőrzésének befejezése után kezdheti meg.

Az ellenőrzés alapján a Hatóság a kezelendő adatok körének, illetőleg az adatfeldolgozás módszerének megváltoztatására hívhatja fel a Társaságot.

IX. FEJEZET

RENDELKEZŐ RÉSZ

1. A szakterületen folyó adatkezelések részletes szabályainak kidolgozása, naprakészen tartása a vonatkozó jogszabályok és jelen Szabályzat előírásai alapján, különös tekintettel a személyes adatok megismerésének, illetve a közérdekű adatok kiadásának rendjére.
Felelős: vezérigazgató-helyettesek, igazgatók, irodavezetők, főosztályvezetők
Határidő: folyamatos, a személyes adatok megismerésének rendjére vonatkozóan 2016. május 1.
2. A hatályos társasági szabályozások adatvédelmet érintő rendelkezéseinek felülvizsgálata, szükség esetén azok módosítása az Infotv.-nek és jelen Szabályzatnak megfelelően. A felülvizsgálatokról, illetve módosításokról a belső ellenőrzési főosztályvezetőt, a jogi és humánpolitikai, és a biztonsági igazgatót írásban tájékoztatni kell.
Felelős: vezérigazgató-helyettesek, igazgatók, irodavezetők, főosztályvezetők
Határidő: 2016. május 1.
3. Valamennyi, a Társaság kezelésében/tulajdonában, stb. lévő kameráról nyilvántartás készítése, elkülönítve a Kivételi Körbe tartozó kamerákat azoktól, melyekkel adatkezelés válik meg, illetve elkülönítve a telephelyi (tehát munkavállalókat), illetve utasforgalmi/járműveken lévő stb. (tehát elsődlegesen utasokat) megfigyelő kamerákat.
Felelős: vezérigazgató-helyettesek, igazgatók
Határidő: 2016. május 1.
4. A BKK Zrt.-vel egyeztetés és annak meghatározása, hogy a már meglévő kamerák vonatkozásában az utastájékoztatási feladatok e körben mely Társaság kötelezettségébe tartoznak.
Felelős: autóbusz és trolibusz üzemeltetési, illetve vasúti üzemeltetési vezérigazgató-helyettesek, jogi és humánpolitikai igazgató
Határidő: 2016. május 1.
5. A személyes adatok kezeléséről szóló tájékoztatók előkészítése és hatósági jóváhagyatása jelen Szabályzat alapján.
Felelős: autóbusz és trolibusz üzemeltetési, illetve vasúti üzemeltetési vezérigazgató-helyettesek, adatvédelmi felelős
Határidő: 2016. május 1.
6. Szükséges a személyes adatok kezelésére vonatkozó tájékoztatás megvalósítása, az ehhez szükséges beszerzések lefolytatása.
Felelős: vezérigazgató-helyettesek
Határidő: 2016. június 1.

7. A jelen Szabályzat évente történő felülvizsgálata, a felülvizsgálat eredményétől függően a Szabályzat módosításának kezdeményezése.
Felelős: adatvédelmi felelős
Határidő: minden év január 31.
8. A Társaságnál működő és ezután létrehozásra kerülő nyilvántartásokkal, adatbázisokkal, adatkezelésekkel kapcsolatban informatikai ágon felelős az adatvédelem és adatbiztonság szabályainak érvényesüléséért.
Felelős: informatikai igazgató
Határidő: folyamatos
9. Az informatikai főosztályvezető évenkénti beszámoltatása, a szakterületek IT-biztonsági helyzetének elemzése a vezérigazgató felé, erről a belső ellenőrzési főosztályvezető, a jogi és a biztonsági igazgató írásbeli tájékoztatása.
Felelős: gazdasági vezérigazgató-helyettes
Határidő: minden év január 31.
10. Az adatvédelemmel összefüggő oktatások megszervezése, lebonyolítása, az adatvédelmi felelőssel együttműködve.
Felelős: jogi és humánpolitikai igazgató
Határidő: folyamatos
11. Az V. fejezetben felsorolt adatvédelmi és adatbiztonsági intézkedések végrehajtásának ellenőrzése és koordinálása.
Felelős: jogi és humánpolitikai igazgató
Határidő: folyamatos
12. Informatikai és egyéb eszközök, dokumentációk, működési feltételek biztosítása az adatvédelmi felelős részére.
Felelős: gazdasági vezérigazgató-helyettes, jogi és humánpolitikai igazgató
Határidő: folyamatos
13. Adatvédelmi ellenőrzések, vizsgálatok kapcsán felmerülő, a Társaságnál használt informatikai rendszerekhez szükséges (ideiglenes) jogosultság-igények soron kívüli, legrövidebb időn belüli beállítása az adatvédelmi felelős részére.
Felelős: gazdasági vezérigazgató-helyettes
Határidő: igény felmerülése esetén azonnal

A Szabályzat a Társaság intranetes honlapján történő megjelenésének napján lép hatályba, egyidejűleg hatályát veszti a „Társasági Adatvédelmi és Adatbiztonsági Szabályzat 2014.” megjelölésű dokumentum.

A szabályozások rendjéről szóló 46/VU/2012. II. fejezet 4. pontjában foglaltak szerint a Szabályzat a Jogi és Humánpolitikai Igazgatóság és a Gazdasági Igazgatóság Informatikai Főosztálya együttes gondozásában jelenik meg.

A Szabályzattal kapcsolatban felvilágosítást a belső adatvédelmi felelős ad a 11-802-es telefonszámon.

2016. „ 04. ” 07.

Bolla Tibor s.k.
elnök-vezérigazgató

Budapesti Közlekedési Zártkörűen Működő Részvénytársaság
Szakigazgatóság

1980 Budapest, Akácfa u. 15. • Tel.: 461-6500 • Fax: 461-6500

.....
Iktatószám:

.....
Ügveintéző:

.....
Telefon:

.....
Kelt:

.....
Melléklet:

TITOKTARTÁSI NYILATKOZAT

Alulírott:

születési hely, idő:

anyja neve:

tudomásul veszem, hogy a Budapesti Közlekedési Zártkörűen Működő Részvénytársaság munkájával 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:,

.....

nyilatkozattevő

.....

munkáltatói jogkört gyakorló

TÖRZSKÖNYV
SZEMÉLYES ADAT KEZELÉSÉRŐL

1. Az adatkezelés

megnevezése:

célja, rendeltetése:

jogsabályi alapja:

időtartama:

2. Az adatok kezelője

szervezeti egység neve:

vezetőjének neve, beosztása:

az adatfeldolgozást végző felelős személy

neve, beosztása:

elérhetősége (telephely, iroda, telefonszám):

3. Az érintettek

köre és száma:

4. A nyilvántartott adatok

köre:

5. Az adatok forrása☐ maga az érintett☐ más adatkezelés**6. Az adatfeldolgozás módszere**☐ manuális☐ számítógépes☐ vegyes**7. Az adatokon végzett gyakori adatkezelési műveletek**☐ tárolás☐ módosítás☐ aktualizálás☐ válogatás☐ rendszerezés

egyéb:

8. Adattovábbítás

mely szerv részére:

milyen rendszerességgel:

9. Adatbiztonsági intézkedések

.....

.....

10. Az adatok

megőrzésének ideje:

törlésének ideje:

JEGYZŐKÖNYV ADATKEZELÉSEK ÖSSZEKAPCSOLÁSÁRÓL

1. Az összekapcsolt adatkezelések

megnevezése:

célja, rendeltetése:

időpontja és tartama:

jogszabályi alapja:

2. Az összekapcsolást végző

szakigazgatóság, szervezeti egység neve:

vezetőjének neve, beosztása:

az összekapcsolást végző felelős személy

neve, beosztása:

elérhetősége (telephely, iroda, telefonszám):

3. Az összekapcsolással érintettek

köre és száma:

4. A összekapcsolt adatok

köre:

5. Az összekapcsolás módszere

☐ manuális

☐ számítógépes

☐ vegyes

6. Adatbiztonsági intézkedések

.....

.....

JEGYZŐKÖNYV
MEGKERESÉS ALAPJÁN TELJESÍTETT ADATSZOLGÁLTATÁSRÓL

1. A megkeresést végző szerv vagy személy

megnevezése:

postacíme:

telefonszáma:

2. Az adatkérés

célja:

rendeltetése:

jogszabályi alapja:

illetve az érintett hozzájáruló nyilatkozata ☐

időpontja:

3. Az adatszolgáltatás alapjául szolgáló

adatkezelés megnevezése:

4. Az adatszolgáltatást teljesítő

szakigazgatóság, szervezeti egység neve:

vezetőjének neve, beosztása:

5. Az érintettek

köre:

6. A továbbított adatok

köre:

7. Az adattovábbítás

módja:

JEGYZŐKÖNYV
KÜLFÖLDRE IRÁNYULÓ ADATSZOLGÁLTATÁSRÓL

1. Az adattovábbítás címzettje

megnevezése:

postacíme:

telefonszáma:

2. Az adattovábbítás

célja:

rendeltetése:

jogszabályi alapja:

illetve az érintett hozzájáruló nyilatkozata ☐

időpontja:

3. Az adatszolgáltatást teljesítő

szakigazgatóság, szervezeti egység neve:

vezetőjének neve, beosztása:

4. Az érintettek

köre:

5. A továbbított adatok

köre:

6. Az adattovábbítás

módja:

1. FÜGGELÉK

KAPCSOLÓDÓ JOGSZABÁLYOK GYŰJTEMÉNYE

- az információs önrendelkezési jogról és információszabadságról szóló 2011. évi CXII. tv. (Infotv.)
- a közérdekű és közérdekből nyilvános adatok közzétételére vonatkozó kötelezettségnek, valamint a köztulajdonban álló gazdasági társaságok takarékosabb működéséről szóló 2009. évi CXXII. tv.
- a minősített adat védelméről szóló 2009. évi CLV. tv.
- a munka törvénykönyvéről szóló 2012. évi I. tv. (Mt.)
- a Polgári Törvénykönyvről szóló 2013. évi V. tv. (Ptk.)
- a foglalkoztatás elősegítéséről, a munkanélküliek ellátásáról szóló 1991. évi IV. tv.
- az adózás rendjéről szóló 2003. évi XCII. tv.
- a személyszállítási szolgáltatásokról szóló 2012. évi XLI. tv. (Sztv.)
- a személyi- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól szóló 2005. évi CXXXIII. tv. (Vtv.)
- a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. tv.
- a személyazonosító jel helyébe lépő azonosítási módokról és az azonosító kódok használatáról szóló 1996. évi XX. tv.
- a kutatás és a közvetlen üzletszerzés célját szolgáló név- és lakcímadatok kezeléséről szóló 1995. évi CXIX. tv.
- az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. tv.
- az elektronikus hírközlésről szóló 2003. évi C. tv.
- a Rendőrségről szóló 1994. évi XXXIV. tv.
- a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. tv.
- a közokiratokról, a közlevéltárakról és a magánlevéltári anyag védelméről szóló 1995. évi LXVI. tv. (Lvtv.)
- az egyének védelméről a személyes adatok gépi feldolgozása során, Strasbourgban, 1981. január 28. napján kelt Egyezmény kihirdetéséről szóló 1998. évi VI. tv.
- a büntető törvénykönyvről szóló 2012. évi C. tv.
- a Nemzetbiztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről szóló 90/2010. (III.26.) Korm. rend.

2. FÜGGELÉK

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

adatifeldolgozás

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;

adatifeldolgozó

az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely szerződés alapján - beleértve a jogszabály rendelkezése alapján kötött szerződést is - adatok feldolgozását végzi;

adatfelelős

az a közfeladatot ellátó szerv, amely az elektronikus úton kötelezően közzéteendő közérdekű adatot előállította, illetve amelynek a működése során ez az adat keletkezett;

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) memóriák (pl. flashdrive)

adatkezelés

az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése;

adatkezelő

az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely önállóan vagy másokkal együtt az adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja;

adatkezelő szervezeti egység

a Társaság azon szervezeti egysége, amely adatkezelést végez

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

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 incidens

személyes adat jogellenes kezelése vagy feldolgozása, így különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés;

adatzárolás

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

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, útlevele száma)

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;

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 ország

minden olyan ország, amely nem tagja az Európai Gazdasági Térségnek

harmadik személy

olyan természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, amely vagy aki nem azonos az érintettel, az adatkezelővel vagy az adatfeldolgozóval

hálózat

számítógépek vagy általánosabban: informatikai rendszerek összekapcsolása, amely az összekapcsolt rendszerek legkülönbözőbb komponensei között adatcserét tesz lehetővé

hozzájárulás

az érintett kívánságának önkéntes és határozott kinyilvánítása, amely megfelelő tájékoztatáson alapul, és amellyel félreérthetetlen beleegyezését adja a rá vonatkozó személyes adatok — teljes körű vagy egyes műveletekre kiterjedő — kezeléséhez

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, akik érvényes szerződéses kapcsolatban állnak a Társasággal és bármilyen informatikai szolgáltatás kialakításában, vagy fenntartásában vesznek részt

jogosultság

számítógépes környezetben a hozzáférési lehetőség megadása valamely tevékenység végrehajtásához

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 terjeszthetők. A közérdekből nyilvános személyes adatok honlapon történő közzétételére az 1. melléklet és 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.

különleges adat

a) a faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviseleti szervezeti tagságra, a szexuális életre vonatkozó személyes adat,

b) az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat, valamint a bűnügyi személyes adat;

nyilvánosságra hozatal

ha az adatot bárki számára hozzáférhetővé teszik

program

eljárési 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

az érintettel kapcsolatba hozható adat - különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret -, valamint az adatból levonható, az érintettre vonatkozó következtetés

személyi számítógép

az IT-Szolgáltató vagy a Társaság tulajdonában álló, önálló vagy hálózati üzemmódú, általában IBM PC kompatibilis asztali számítógép vagy hordozható eszköz (pl. laptop, táblagép)

szoftver

valamely informatikai rendszer olyan logikai része, amely a működtetés vezérléséhez szükséges

tiltakozás

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