BUDAPESTI
KÖZLEKEDÉSI
KÖZPONT

36/2014. sz. Vezérigazgatói utasítás

a BKK Zrt. adatvédelmi és adatbiztonsági szabályzatáról

BKK Budapesti Közlekedési Központ
Zártkörűen Működő Részvénytársaság
cégjegyzékszám: 01-10-046840
cím: 1075 Budapest, Rumbach Sebestyén utca 19-21.

telefonszám: +36 30 774 1000
fax: +36 30 774 1001
web: www.bkk.hu
e-mail: bkk@bkk.hu
iktató szám: 1167/109-1/2014/1167

BEVEZETÉS

A BKK Budapesti Közlekedési Központ Zártkörűen Működő Részvénytársaság szabályzatkezelés rendjéről szóló 16/2014 sz. Vezérigazgatói utasítás 7) pontja alapján a következőket rendelem el:

1. ÁLTALÁNOS RENDELKEZÉSEK

1.1. A szabályzat célja és hatálya

1) A jelen szabályzat célja, hogy meghatározza a BKK Zrt. adatvédelmi és adatbiztonsági tevékenységének szabályait.

2) A szabályzat személyi hatálya kiterjed a BKK Zrt. valamennyi szervezeti egységére, és munkavállalójára. A BKK Zrt.-vel szerződéses kapcsolatban álló, munkavégzésre irányuló vagy egyéb, a Szabályzat tárgyi hatálya alá tartozó tevékenységet is érintő jogviszonyban álló személyekre a szabályzat alkalmazásának kötelezettségét az ezen személyekkel kötött szerződésben elő kell írni.

3) A szabályzat tárgyi hatálya kiterjed a BKK Zrt. szervezeti egységei által kezelt valamennyi személyes adatra, a rajtuk végzett adatkezelési műveletek teljes körére, keletkezésük, kezelésük, feldolgozásuk helyétől, valamint megjelenési formájuktól függetlenül.

2. RÉSZLETES SZABÁLYOK

4) A BKK Zrt. adatvédelmi és adatbiztonsági szabályait a jelen vezérigazgatói utasítás 1 számú melléklete tartalmazza.

3. ZÁRÓ RENDELKEZÉSEK

5) A jelen szabályzat az aláírásának napját követő 3. munkanapon lép hatályba.

6) A szabályzat rendelkezéseit a folyamatban lévő ügyekben is alkalmazni kell.

2014. október 29

Vitézy Dávid
vezérigazgató

4. Mellékletek

1. számú melléklet: A BKK ZRT. ADATVÉDELMI ÉS ADATBIZTONSÁGI SZABÁLYZATA

1. számú melléklet a 36/2014 sz. Vezérigazgatói utasításhoz

ADATVÉDELMI ÉS ADATBIZTONSÁGI SZABÁLYZAT

I. BEVEZETŐ RENDELKEZÉSEK

1. *Az Adatvédelmi és Adatbiztonsági Szabályzat célja, hatálya*

1.1. Az Adatvédelmi és Adatbiztonsági Szabályzat (a továbbiakban: Szabályzat) célja, hogy meghatározza a BKK Zrt.-nél zajló adatkezelések törvényes keretét, biztosítsa az adatvédelem alkotmányos elveinek és az információs önrendelkezési jognak az érvényesítését, elősegítse az adatbiztonság követelményeinek való megfelelést, továbbá megakadályozza a jogosulatlan adatkezelést. Az Adatvédelmi és Adatbiztonsági Szabályzat kialakítja az adatvédelem szempontjából fontos feladatokat, felelősségi viszonyokat, különös tekintettel a munkavállalók szerepére az adatbiztonságban.

1.2. Jelen Szabályzat hatálya kiterjed a BKK Zrt. székhelyén és telephelyein, valamint szolgáltatási helyszínein és eszközein folyó valamennyi adatkezelésre, adattovábbításra, információ-átadásra, az ezen adatkezelés, információátadás tárgyát képező adat jelen Szabályzatban meghatározottak szerinti, üzleti titokként történő kezelésével és védelmével kapcsolatos tevékenységekre.

1.3. A Szabályzat személyi hatálya kiterjed a BKK Zrt. valamennyi szervezeti egységére, és munkavállalójára. A BKK Zrt.-vel szerződéses kapcsolatban álló, munkavégzésre irányuló vagy egyéb, a Szabályzat tárgyi hatálya alá tartozó tevékenységet is érintő jogviszonyban álló személyekre a szabályzat alkalmazásának kötelezettségét az ezen személyekkel kötött szerződésben elő kell írni.

1.4. A Szabályzat tárgyi hatálya kiterjed a BKK Zrt. szervezeti egységei által a BKK Zrt. székhelyén és telephelyein, valamint szolgáltatási helyszínein és eszközein kezelt valamennyi személyes adatra, a rajtuk végzett adatkezelési műveletek teljes körére, keletkezésük, kezelésük, feldolgozásuk helyétől, valamint megjelenési formájuktól függetlenül.

2. *Jogszabályi alap, kapcsolat az adatkezelő belső szabályzataival*

2.1 Jelen Szabályzat jogszabályi alapját a következő törvények jelentik:

- Magyarország Alaptörvénye;
- 2011. évi CXII. törvény – az információs önrendelkezési jogról és az információszabadságról (a továbbiakban: Infotv.);
- 2013. évi V. törvény – a Polgári Törvénykönyvről (a továbbiakban: Ptk.);
- 2012. évi C. törvény a Büntető Törvénykönyvről;
- 1996. évi LVII. törvény - a tisztességtelen piaci magatartás és a versenykorlátozás tilalmáról.

2.2. Jelen Szabályzat a BKK Zrt. belső szabályzataival együtt értelmezendő, így különösen az alábbiakkal:

- Szervezeti és Működési Szabályzat
- Ügyrend
- Biztonságvédelmi Szabályzat
- Információbiztonsági Szabályzat
- Közérdekű adatok közzétételének rendjéről szóló Szabályzat

3. Értelmező rendelkezések

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

3.2. *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 abból levonható, az érintettre vonatkozó következtetés;

3.3. *különleges adat:* 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, az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat, valamint a bűnügyi személyes adat;

3.4. *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;

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

3.6. *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 általa megbízott adatfeldolgozóval végrehajtatja;

3.7. *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;

3.8. *adattovábbítás*: az adat meghatározott harmadik személy számára hozzáférhetővé tétele;

3.9. *nyilvánosságra hozatal*: az adat bárki számára történő hozzáférhetővé tétele;

3.10. *adattörlés*: az adatok felismerhetetlenné tétele oly módon, hogy a helyreállításuk többé nem lehetséges;

3.11. *adatmegjelölés:* az adat azonosító jelzéssel ellátása annak megkülönböztetése céljából;

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

3.13. *adatmegsemmisítés*: az adatokat tartalmazó adathordozó teljes fizikai megsemmisítése;

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

3.15. *adatfeldolgozó*: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki, vagy amely az adatkezelővel kötött szerződése alapján – beleértve a jogszabály rendelkezése alapján történő szerződéskötést is – az adatok feldolgozását végzi;

3.16. *harmadik személy*: olyan természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely nem azonos az érintettel, az adatkezelővel vagy az adatfeldolgozóval;

3.17. *harmadik ország*: minden olyan ország, amely nem tagja az Európai Gazdasági Térségnek;

3.18. *üzleti titok*: a gazdasági tevékenységhez kapcsolódó minden olyan tény, információ, megoldás vagy adat, amelynek nyilvánosságra hozatala, illetéktelenek által történő megszerzése vagy felhasználása a jogosult - ide nem értve a magyar államot - jogszerű pénzügyi, gazdasági vagy piaci érdekeit sértené vagy veszélyeztetné, és amelynek titokban tartása érdekében a jogosult a szükséges intézkedéseket megtette.

4. Az adatkezelő

4.1. Az adatkezelő adatai:
Név: BKK Budapesti Közlekedési Központ Zártkörűen Működő Részvénytársaság
Székhely: 1075 Budapest, Rumbach Sebestyén utca 19-21.
Cégjegyzékszám: 01-10-046840
Cégbejegyzés: Fővárosi Bíróság, mint Cégbíróság
Belső adatvédelmi felelős neve: *folyamatban*
Elérhetősége: bkk@bkk.hu

4.2. Adatkezelések
Az egyes adatkezelések részletes leírása, valamint azok nyilvántartási számai és feltételei a jelen Szabályzattal együttesen értelmezendő adatkezelési tájékoztatókban (a továbbiakban: Adatkezelési Tájékoztató) kerülnek elhelyezésre.

II. ADATVÉDELEM

5. *Adatkezelőre és adatkezelésre vonatkozó szabályok*

5.1. Az adatvédelmi szabályok betartásáért az adatkezelő a felelős. Az adatkezelő szervezet munkavállalója az adatvédelmi és adatbiztonsági szabályok betartásáért személyes felelősséggel tartozik.

5.2. Az adatkezelő személyes adatokat csak az Infotv. 5. §-ában meghatározott felhatalmazás alapján kezelhet, nevezetesen

a) az érintett hozzájárulásával, vagy

b) törvény vagy - törvény felhatalmazása alapján, az abban meghatározott körben - helyi önkormányzat rendelete közérdeken alapuló célból elrendeli (kötelező adatkezelés).

Az Infotv. 6. §-ában foglaltak alapján személyes adat akkor is kezelhető, ha az érintett hozzájárulásának beszerzése lehetetlen vagy aránytalan költséggel járna, és a személyes adat kezelése az adatkezelőre vonatkozó jogi kötelezettség teljesítése céljából szükséges, vagy az adatkezelő vagy harmadik személy jogos érdekének érvényesítése céljából szükséges, és ezen érdek érvényesítése a személyes adatok védelméhez fűződő jog korlátozásával arányban áll.

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

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.

5.3. Az érintett kérelmére indult eljárásban, az annak lefolytatásához szükséges adatainak kezeléséhez való hozzájárulását vélelmezni kell. Erre a tényre az érintett figyelmét fel kell hívni.

5.4. Az érintett az adatkezeléshez való hozzájárulását kizárólag részletes és egyértelmű tájékoztatás birtokában adhatja meg, amelyről az adatkezelő feladata gondoskodni.

5.5. Személyes adatot kezelni csak meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében lehet. Az adatkezelésnek minden szakaszában meg kell felelnie e kritériumoknak.

5.6. Csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas, csak a cél megvalósulásához szükséges mértékben és ideig.

5.7. Az adatkezelő köteles gondoskodni a kezelésében lévő adatok minőségéről, így különösen azok pontosságáról, teljességéről és időszerűségéről.

6. Feladatok az adatkezelések során

6.1. A belső adatvédelmi felelős
Az adatkezelő erre feljogosított vezetője a jelen Szabályzat érvényesítése érdekében belső adatvédelmi felelőst nevez ki.

A belső adatvédelmi felelős

a) szakmai szempontból irányítja, felügyeli, ellenőrzi a BKK Zrt. adatvédelmi tevékenységét;

b) ellenőrzi a jogszabályok, valamint a jelen Szabályzat rendelkezéseinek a megtartását;

c) kivizsgálja a hozzá érkezett bejelentéseket, jogosulatlan adatkezelés esetén annak megszüntetésére hívja fel az adatkezelőt;

d) az adatkezelőhöz külső szervektől és személyektől érkező megkereséseket véleményezi, majd további intézkedés végett megküldi az adatok kezelésére és átadására jogosult szervezeti egységhez, szakterülethez;

e) a megkeresésekről, azok teljesítéséről vagy elutasításáról nyilvántartást vezet, amelynek megőrzési ideje öt év;

f) felülvizsgálja és aktualizálja a jelen Szabályzatot;

g) gondoskodik az adatkezeléseknek az adatvédelmi nyilvántartásba történő bejelentéséről;

h) vezeti a belső adatvédelmi nyilvántartást;

i) a humánpolitikai feladatokat ellátó szervezeti egységgel együttműködve gondoskodik az adatvédelmi ismeretek oktatásáról.

6.2. A szervezeti egységek vezetői

a) felelősek az irányításuk alá tartozó szervezeti egység adatkezeléseinek jogszabályoknak és jelen Szabályzatnak való megfelelőségéért,

b) felelősek azért, hogy az általuk vezetett szervezeti egység adatkezelései során a jelen Szabályzat 14. fejezetében foglalt adatbiztonsági előírások maradéktalanul teljesüljenek,

c) ellenőrzik az adatvédelemmel kapcsolatos előírások, így különösen jelen Szabályzat rendelkezéseink betartását.

6.3. Az adatkezelést végző személy

A BKK Zrt. szervezetén belül adatkezelést végző személy a tevékenységi körén belül felelős az adatok feldolgozásáért, megváltoztatásáért, törléséért, továbbításáért és nyilvánosságra hozataláért, valamint az adatok pontos, követhető dokumentálásáért.

Az adatkezelést végző személy tevékenysége során:

a) kezeli és megőrzi a feladata ellátása során birtokába került adatokat,

b) ügyel a személyes adatokat tartalmazó nyilvántartások biztonságos kezelésére és tárolására,

c) gondoskodik arról, hogy az általa kezelt adatokhoz illetéktelen személy ne férhessen hozzá,

d) betartja az adatkezelésre vonatkozó jogszabályokat és szabályzatokat,

e) részt vesz az adatkezeléssel, adatvédelemmel összefüggő oktatásokon.

7. Az adatok tárolása

7.1. A kezelt adatokat úgy kell tárolni, hogy azokhoz illetéktelenek – ide értve azon munkavállalókat is, akik nem jogosultak ezen adatok megismerésére, kezelésére – ne férhessenek hozzá.

7.2. Az adatok informatikai módszerrel történő tárolási módját úgy kell megválasztani, hogy azok törlése – az esetleg eltérő törlési határidőre is tekintettel – az adattörlési határidő lejártakor, illetve ha az egyéb okból szükséges, elvégezhető legyen. A törlésnek visszaállíthatatlannak és ellenőrizhetőnek kell lennie.

8. Az adatok felhasználása

8.1. A BKK Zrt. által kezelt adatok kizárólag a hatályos Adatkezelési Tájékoztatókban meghatározott célokra használhatók fel.

8.2. Számítástechnikai, távközlési eszközök és programok helyességének ellenőrzésére, felhasználók betanítására, illetve oktatási célra valós személyi adatokat felhasználni nem lehet.

8.3. A BKK Zrt. által kezelt adatok nyilvánosságra hozatala tilos, kivéve, ha azt törvény rendeli el.

8.4. A 8.3. pontban foglalt tilalom nem érinti az adatkezelőről szóló statisztikai adatokat, amelyek korlátozás nélkül nyilvánosságra hozhatók.

9. Az adatok feldolgozása

9.1. A személyes adatokon technikai műveletet az adatkezelő alvállalkozója adatfeldolgozóként az érintett hozzájárulása nélkül is végrehajthat, amennyiben tevékenysége során önálló érdemi döntést nem hoz.

9.2. A BKK Zrt. harmadik személy kezelésében lévő személyes adatokon – amennyiben e tevékenysége során érdemi döntési jogkörrel nem rendelkezik – adatfeldolgozóként az érintett hozzájárulása nélkül is végezhet technikai műveleteket.

9.3. Az adatkezelő köteles az érintetteket tájékoztatni – lehetőleg már az adatfelvételkor – az igénybe vett adatfeldolgozók személyéről.

9.4. Az adatfeldolgozásra vonatkozó megbízást írásba kell foglalni. A szerződésnek a következő elemeket kell tartalmaznia:

a) az adatkezelő és az adatfeldolgozó megnevezését;

b) az adatfeldolgozási tevékenység megnevezését;

c) az átadandó adatok körét;

d) az adatkezelő szavatolását az adatbázis jogszerű kezeléséért;

e) az adatfeldolgozó nyilatkozatát, hogy kizárólag az adatkezelő utasítása alapján végzi az adatok feldolgozását;

f) az adatfeldolgozónak a saját és a szerződésben foglaltaktól eltérő célú adatfelhasználásának tilalmát;

g) az adatfeldolgozó kötelezettségvállalását az adatbiztonsági szabályok megtartására;

h) az adatok sorsára vonatkozó rendelkezést a szerződés megszűnésének eseteire;

i) mindezekért való anyagi felelősségvállalást.

9.5. Az adatfeldolgozó részére csak olyan személyes adatok adhatók át, amelyek szerepelnek

a) az adatfeldolgozói szerződésben,

b) és az Adatkezelési Tájékoztatóban vagy a konkrét adatkezelésre vonatkozó egyéb tájékoztatásban.

9.6. Az adatfeldolgozói feladat teljesítését követően, illetve a szerződés megszűnésekor az adatfeldolgozó a birtokában lévő személyes adatokat vissza kell, hogy szolgáltassa az adatkezelőnek. Az átadott adatok adatfeldolgozó számítástechnikai rendszerében található másolatait pedig visszavonhatatlan módon töröltetni kell, amelynek megtörténtéről az adatfeldolgozónak nyilatkoznia kell.

10. A személyes adatok törlése, helyesbítése

10.1. Az adatokat törölni - manuális nyilvántartás esetén megsemmisíteni - szükséges, ha

a) az adatkezelésre a tájékoztatóban előírt határidő eltelt;

b) az adatkezelés jogszerűtlensége megállapítást nyert;

c) az érintett hozzájárulását visszavonta, kivéve, ha törvény az adatok további kezelését lehetővé teszi;

d) az adatkezelés célja megszűnt;

e) az adatvédelmi hatóság vagy bíróság jogerős határozattal elrendelte.

10.2. Az érintett bejelentése vagy az adatkezelő által észlelt hibás adat esetén az adatkezelő a hibás adatot helyesbíti.

10.3. Ha a hibás adat nem helyesbíthető, akkor törölni kell. Amennyiben a törlés vagy a helyesbítés az adatok tárolási módja miatt nem lehetséges, akkor az adatot megfelelő helyesbítő vagy figyelemfelhívó feljegyzés hozzáfűzésével véglegesen zárolni kell.

10.4. 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.

10.5. Ha az adat hibás volta annak továbbítása után derül ki, akkor ennek tényéről, illetve - amennyiben a hibás adatot az adatkezelő kijavította - a helyes adatról mindazokat tájékoztatni kell, akiknek az adatot továbbították. A tájékoztatás mellőzhető, ha ez az adat jellegére, az adatkezelés céljára, az időmúlásra, illetve az adatkezeléssel

összefüggő más körülményeire tekintettel az érintett, illetve a korábbi adattovábbítás címzettjének jogos érdekét nem sérti.

11. Adattovábbítási nyilvántartás

11.1. Az adatkezelő a kezelt személyes adat továbbításáról nyilvántartást vezet, amely tartalmazza:

a) az adattovábbítás célját, jogalapját, időpontját;

b) az adatigénylő azonosításához szükséges adatokat;

c) a továbbított adatfajták megnevezését.

11.2. Az adattovábbítási nyilvántartásba betekinthet, abból adatot igényelhet:

a) az adatvédelmi hatóság, a bíróság, nyomozó hatóság, a nemzetbiztonsági szerv, törvényben meghatározott feladatai ellátásához,

b) az adatkezelő szervezet vezetője, vagy az általa meghatalmazott személy.

11.3. Az adattovábbítási nyilvántartásba való betekintést, az abból történő adattovábbítást dokumentálni kell.

11.4. Az adattovábbítási nyilvántartás vezetési kötelezettségének eleget lehet tenni az elektronikus úton történt adattovábbítás naplózásával is.

11.5. Az adattovábbítási nyilvántartást 5 évig, különleges adat továbbítása esetében 20 évig kell visszakereshető módon megőrizni.

12. Az érintett jogai gyakorlásának biztosítása

12.1. Az érintett az adatkezelés ideje alatt az adatkezelőtől tájékoztatást kérhet személyes adatai kezeléséről, valamint azokba betekintést nyerhet. A betekintés jogát oly módon kell biztosítani, hogy az érintett más személy adatait ne ismerhesse meg.

12.2. Az érintett kérelmére az adatkezelő tájékoztatást ad az általa kezelt adatairól, az adatkezelés céljáról, jogalapjáról, időtartamáról, az adatkezelésre, valamint az adatfeldolgozásra jogosult személyéről, továbbá arról, hogy kik és milyen célból ismerhetik, ismerték meg az adatokat.

12.3. Téves adatrögzítés vagy adatváltozás esetén az érintett Infotv. 14. § b) pontja alapján benyújtott kérelmére az adatkezelő a hibásan kezelt személyes adatokat helyesbíti. Ha az adat helyesbítése nem lehetséges, vagy az adatkezelő az adatot törvényes felhatalmazás, illetve az érintett hozzájárulása nélkül kezeli, akkor az adatot törölni, illetve véglegesen zárolni kell.

12.4. A helyesbítési, törlési kérelmet érdemben meg kell vizsgálni, és amennyiben az megalapozott, a helyesbítést, törlést teljesíteni kell, attól függetlenül, hogy az érintett tájékoztatható-e az eljárás eredményéről.

12.5. Az érintett adatainak helyesbítésére, illetve törlésére irányuló eljárásra az Infotv. rendelkezéseit kell alkalmazni.

12.6. A kijavításról és a törlésről az érintettet és az Infotv. 18. § szerinti szerveket az ott meghatározottak szerint, az Infotv. 19. §-ára is figyelemmel kell értesíteni.

III. ADATBIZTONSÁG

13. A számítástechnikai rendszerben tárolt adatok biztonsága

13.1. Jelen Szabályzat alapvető rendeltetése a személyes adatok és az üzleti titokká minősített adatok megismerhetőségének korlátozására vonatkozó szabályok kialakítása, illetve ezen adatok illetéktelen személyek általi megismerhetőségének megakadályozása.

13.2. A fenti cél elérése érdekében az adatkezelések során - az adatkezelés jellegétől függően - az információ-rendszerek következő védelmi módszereit kell alkalmazni:

a) Ügyviteli védelem: a számítástechnikai-rendszer felelőseinek (IT) és az adatkezeléssel kapcsolatos tevékenységnek szervezési és adminisztratív módon történő nyomon követése, a felelősség körülhatárolása. Kiterjed az informatikai rendszerre és annak szolgáltatásaira, valamint az adathordozók kezelésére, beleértve a hozzáférési jogosultság és a betekintés dokumentálását is.

b) Fizikai védelem: olyan eszközök alkalmazása, amelyekkel azok a helyiségek védhetők, ahol számítástechnikai erőforrásokat használnak, vagy az adatmegőrzés szempontjából fontosak. Az információs rendszer minősítésétől függő védelemben kell részesíteni az adathordozókat is.

c) Algoritmikus védelem: matematikai algoritmusok alapján működő védelem, amely az egyedi számítógépen és a hálózaton is lehetővé teszi a használó azonosítását, a jogosultság ellenőrzését.

13.3. A fizikai biztonság megteremtéséhez az alábbi intézkedéseket szükséges megtenni:

a) Az adathordozó eszközök elhelyezésére szolgáló helyiségeket (épületeket, épületrészeket) úgy kell kialakítani, hogy elegendő biztonságot nyújtsanak illetéktelen vagy erőszakos behatolás, tűz vagy természeti csapás ellen.

b) Azokba a helyiségekbe, ahol adatkezelés folyik, a személyek belépését - a minősítéstől függően - korlátozni és ellenőrizni kell. A belépésre adott felhatalmazásnak összhangban kell lennie az adott személy hivatalos feladataival, illetőleg az ott kezelt adatokhoz történő hozzáférési jogosultságával.

c) A számítástechnikai eszközzel olvasható és a manuális adathordozók tárolását, hozzáférését és felhasználását ellenőrizni kell. Különös figyelmet kell fordítani arra, hogy a biztonságos területről kivitt eszközök maradványadatokat ne tartalmazzanak.

d) Az adathordozókról és mozgásukról, azok tartalmáról és felhasználásáról nyilvántartást kell vezetni.

e) A kezelt adatokat a BKK Zrt. szempontjából vett értékükkel és érzékenységükkel kifejezve kell differenciálni, osztályokba sorolni. Minden egyes osztályba sorolási eljáráshoz információkezelési eljárást is meg kell határozni annak érdekében, hogy azok a következő információfeldolgozási tevékenységfajtákat lefedjék:

- a másolást;
- a tárolást;
- a továbbítást postai úton, faxon és elektronikus levelezéssel;
- a beszélt szavakkal való átvitelt, beleértve a mobiltelefont, a hangüzenet szolgáltatást, valamint az üzenetrögzítést;

- a megsemmisítést.

f) Annak érdekében, hogy lecsökkenjen a jogosulatlan hozzáférés, az információvesztés és információrongálás kockázata, mind a rendes munkaidőben, mind azon kívül, bevezetésre kerül az „üres asztal" szabály a papíralapú anyagokra és a hordozható adattárolókra, valamint a „tiszta képernyő" szabály az információfeldolgozó eszközökre. E szabályok részletesen:

- a papíranyagokat és a számítógépek adathordozóit megfelelő, zárható szekrényben vagy más, hasonlóan biztonságos bútorban kell tárolni, amikor éppen nincsenek használatban, különösen a munkaidőn kívüli időszakokban,
- személyi számítógépeket, munkaállomásokat, nyomtatókat és fénymásolókat nem szabad „bejelentkeztetni", amikor felügyelet nélkül maradnak, és azok használaton kívül kulcsreteszekkel, jelszavakkal vagy más óvintézkedésekkel legyenek védve,
- a bejövő és kimenő levelező eszközöket, a felügyeletlen faxgépeket védeni kell,
- fénymásoló gépekhez történő hozzáférést korlátozni, valamint naplózni kell,
- a személyes adat és az üzleti titok kategóriájába sorolt információt kinyomtatás vagy sokszorosítás után azonnal el kell távolítani a nyomtatóról és a fénymásolóból.

g) Az üzleti titoknak minősített adatokat tartalmazó informatikai rendszerekből történő nyomtatásokat az egyéb hozzáférésekhez hasonlóan naplózni kell.

13.4. Az üzemeltetési biztonság kialakítására az alábbi intézkedéseket szükséges megtenni:

a) A számítástechnikai eszközöket üzemeltető személyek feladatait egyértelműen meg kell határozni. Egyéb, a feladatoktól eltérő tevékenységet csak külön, erre irányuló egyedi vezetői felhatalmazás alapján lehet végezni.

b) A hozzáférés jelszavait időközönként, az üzemeltető személyének megváltozása esetén haladéktalanul, de legkésőbb 24 órán belül meg kell változtatni. Jelszót ismételten nem lehet kiadni.

c) A számítástechnikai eszközök előre nem látható üzemzavara esetére olyan tervet kell kidolgozni, amellyel annak hatása ellensúlyozható.

d) A számítástechnikai eszközök felhasználói kötelesek

- az aktív keresési folyamatok lezárására, ha a munka befejeződött, hacsak alkalmas reteszelő mechanizmussal nem tehetők biztonságossá, például jelszóval védett képernyővédővel;
- kijelentkezni, amikor a keresési folyamatokat befejezték (nem elegendő ilyenkor a PC vagy munkaállomás egyszerű kikapcsolása);
- a PC-t, a terminált vagy a munkaállomást, ha az nincs használatban, a jogosulatlan használattal szemben tegyék biztonságossá úgy, hogy kulcsra zárják, vagy ezzel egyenértékű védőintézkedést tesznek, például jelszavas hozzáférést használnak.

13.5. A technikai biztonság érdekében szükséges intézkedések:

a) Az adatok biztonságát szolgáló intézkedések meghatározásakor és alkalmazásakor tekintettel kell lenni a technika mindenkori fejlettségére. Több lehetséges adatkezelési megoldás közül azt kell választani, amely a személyes adatok magasabb szintű védelmét biztosítja, kivéve, ha az aránytalan nehézséget jelentene az adatkezelőnek.

b) Az adatok és programok véletlen vagy szándékos megrongálását számítástechnikai módszerekkel is meg kell akadályozni.

c) Az adatállományok tartalmát képező adattételek számát folyamatosan ellenőrizni kell.

d) Az adatállományok kezelését úgy kell megszervezni, hogy részleges vagy teljes megsemmisülésük esetén tartalmuk rekonstruálható legyen, ennek érdekében az adatállományokról rendszeresen biztonsági másolatot kell készíteni, és azt az eredeti adatállománytól lehetőleg földrajzilag is eltérő helyen, biztonságosan kell tárolni.

A kezelt személyes adatok elvesztésének megakadályozása érdekében a hálózati kiszolgálón (szerver) tárolt adatokat meghatározott időközönként le kell menteni, és a mentéseket tőle fizikailag különböző adattárolón, földrajzilag is elkülönítve kell elhelyezni.

Mind a biztonsági másolathoz, mind a szerver adatállományainak másolataihoz kizárólag az eredeti állományok részleges vagy teljes megsemmisülése, illetőleg katasztrófa esetén lehet hozzáférni.

e) Az adatokhoz és a számítástechnikai eszközökhöz való hozzáférést jelszavakkal kell ellenőrizni.

f) Az adatok és az adatállományok változását naplózni kell.

g) Az adatkezelő programok jogtisztaságát és előírásszerű működését ellenőrizni kell, ideértve a biztonsági vizsgálatot is.

h) Programfejlesztés vagy -próba céljára valódi adatok felhasználását, különösen, ha a próbát külső szervezet vagy személy végzi, el kell kerülni (valós személyes adatok felhasználása nem megengedett).

i) Az adatbevitel során a bevitt adatok helyességét ellenőrizni kell.

j) Közvetlen adathozzáférés kezdeményezésének jogosultságát ellenőrizni kell.

k) Számítástechnikai módszerekkel meg kell akadályozni, hogy az adatokat tároló, hálózatokon keresztül elérhető szerverekhez illetéktelenek hozzáférhessenek.

l) Az adatbiztonsági programokat úgy kell megszerkeszteni, hogy az adatokhoz vagy az adatkezelő programokhoz való illetéktelen hozzáférés kísérletét is jelezzék, naplózzák, illetőleg többszöri ilyen kísérlet esetén a hozzáférést megakadályozzák.

m) Pontosan meg kell határozni (munkakörönként, illetve személyenként) az egyes adatokhoz való hozzáférést.

n) Az adathozzáféréseknél csak azon munkavállalók hozzáférése legyen megadva, akik azzal dolgoznak.

o) Ha központi szerver van, akkor a munkaállomásoknak csak korlátozott, a munkához szükséges jogosultság adható.

p) A Társaság adatokat, adatbázisokat kezelő számítástechnikai eszközein gondoskodni kell a megfelelő vírusvédelemről és vírusmentesítésről;

q) Automatizált adatfeldolgozás esetén naplózni kell, hogy mely személyes adatokat, mikor és ki vitte be az automatizált adatfeldolgozó rendszerbe.

14. Hozzáférési jogosultság

14.1. A BKK Zrt. munkavállalói és alvállalkozói csak olyan személyes adatokhoz férhetnek hozzá, és kizárólag olyan mértékben, amely feladatuk ellátásához elengedhetetlenül szükséges, és csak abban az esetben, ha az adatkezelés egyéb feltételei tekintetükben is fennállnak.

14.2. A hozzáférési jogosultság szabályozásának alapját a személyes adatot és az üzleti titkot képező adat iránti szervezeti, működési igények feltárása jelenti. Minden olyan személy esetében, akinek a vizsgálat alapján a munkájához szükséges a személyes, illetve az üzleti titokká minősített adat, meg kell vizsgálni, hogy adottak-e az üzleti titok és a személyes adat védelméhez szükséges, jelen Szabályzatban előírt feltételek. Ezek hiánya esetén a hozzáférési jogosultság nem engedélyezhető.

14.3. A hozzáférési jogosultságok kiosztásánál meg kell határozni a betöltött munkakör által meghatározott feladatok elvégzéséhez szükséges adatok körét.

14.4. Amennyiben a feltételek adottak, a hozzáférési jogosultságot az érintett munkavállaló szervezeti egységének mindenkori vezetője jogosult megadni, és erről a jogosultságról haladéktalanul tájékoztatja a belső adatvédelmi felelőst. A hozzáférési jogosultság visszavonásig érvényes.

14.5. Az informatikai rendszerekben a hozzáférési jogosultság megadásakor kerül beállításra az, hogy a munkavállaló milyen adathoz, adatállományokhoz férhet hozzá, és azokkal milyen műveleteket végezhet (olvasás, írás, programvégrehajtás, állománymentés, törlés).

14.6. Az adatbázisban, informatikai rendszerekben tárolt személyes adatokat és üzleti titok minősítésű elektronikus adatokat tartalmazó adatállományt illetéktelen hozzáférés, betekintés ellen a folyamat megkezdéséhez szükséges hozzáférési jelszóval kell ellátni.

14.7. Minden személyes adat és üzleti titokká minősített elektronikus adat kezelését támogató informatikai rendszerben, alkalmazásban biztosítani kell a betekintések naplózásának lehetőségét, az alábbi adatokkal:

- a felhasználói azonosítókat (ID);
- a bejelentkezés és kijelentkezés dátumát és időpontját;
- a terminálazonosítót, és ha lehet, a helyet;
- a sikeres és a sikertelen rendszer-hozzáférési kísérletekről készült feljegyzéseket;
- a sikeres és a sikertelen adathozzáférési és más erőforrás-elérési kísérletekről készült feljegyzéseket.

14.8. Amennyiben egy hozzáférési jogosultsággal rendelkező személy észleli, hogy hozzáférési jogosultsága nagyobb, mint amennyire munkája ellátásához szükséges lenne, haladéktalanul értesíteni köteles a szervezeti egysége szerinti vezetőjét és a belső adatvédelmi felelőst.

14.9. A hozzáférési szinteket legalább évente, de minden változtatást követően rendkívülien is felül kell vizsgálni, és a valós szükségletekhez kell igazítani.

15. Munkavállalói adatbiztonsági kötelezettségek

15.1. Aki a személyes adat és az üzleti titkot képező adat megismerésére jogosult:

a) köteles az üzleti titok és a személyes adatok védelmére vonatkozó rendelkezéseket, valamint a jelen Szabályzatban meghatározott előírásokat megismerni, erről írásban nyilatkozni, valamint ezen előírásokat alkalmazni;

b) a tudomására jutott személyes adatot és üzleti titkot az érvényességi időn belül illetéktelen személynek át nem adhatja, illetve nem hozhatja illetéktelen tudomására vagy nyilvánosságra (titoktartási kötelezettség);

c) köteles a hozzáférési jog megszűnésekor – ideértve a munkaviszony megszűnésének eseteit is – az üzleti titokká minősített adatot és a személyes adatot tartalmazó minden nála lévő adathordozót a BKK Zrt.-nek, mint az adattal rendelkező jogosultnak, illetve adatkezelőnek haladéktalanul átadni.

15.2. Személyhez fűződő jogokat sért az a személy, aki üzleti titok birtokába jut, és azt jogosulatlanul nyilvánosságra hozza vagy azzal egyéb módon visszaél.

15.3. Üzleti titok tisztességtelen módon való megszerzésének minősül az is, ha az üzleti titkot a jogosult hozzájárulása nélkül, a vele – a titok megszerzése idején vagy azt megelőzően – bizalmi viszonyban (így különösen a munkaviszony és a munkavégzésre irányuló egyéb jogviszony) vagy üzleti kapcsolatban álló személy közreműködésével szerezték meg.

15.4. A BKK Zrt. valamennyi munkavállalója munkavégzése során köteles jelen Szabályzat rendelkezéseinek, előírásainak érvényt szerezni.

16. Titoktartási kötelezettség

16.1. A BKK Zrt.-vel munkavégzésre irányuló jogviszonyban lévő személyek kötelesek jelen Szabályzat, továbbá a hatályos jogszabályok szerint a rájuk bízott, illetve tudomásukra jutott személyes adatokat és üzleti titkokat megőrizni. A munkavállalók kizárólag a munkaköri leírásban meghatározott feladatkörükön belül ismerhetik meg az ilyen adatokat. E titoktartás nem terjed ki a közérdekű adatok nyilvánosságára és a közérdekből nyilvános adatra vonatkozó, külön törvényben meghatározott adatszolgáltatási és tájékoztatási kötelezettségre.

16.2. Az adatbiztonság személyi feltételeinek kialakítása tekintetében a szervezeti rendszer minden tagját, aki feladatai ellátása során személyes adatot vagy üzleti titkot kezel, megfelelő felkészítésben, oktatásban kell részesíteni.

16.3. Minden személyes vagy üzleti titoknak minősített adatot tartalmazó rendszerhez való hozzáférésre feljogosított munkavállaló köteles teljes bizonyító erejű magánokiratba foglalt titoktartási kötelezettség vállalást tenni. A kötelezettségvállalásban nyilatkozni kell arról, hogy a munkavállaló jelen Szabályzat rendelkezéseit megismerte, azokat magára nézve kötelezőként elismeri, a szükséges titokvédelmi ismereteket elsajátította, valamint a személyes adatok védelméhez fűződő jog és az üzleti titok megsértésének mind büntetőjogi, mind polgári jogi következményeivel tisztában van.

17. A jogellenes adatkezelés következményei

17.1. A személyes adatok kezelésére, valamint az adatok biztonságát szolgáló intézkedések megtételére vonatkozó jogszabályi kötelezettségek megszegése esetén a hatályos Btk. alapján a szabályokat megsértő büntetőjogi felelősségre vonására kerülhet sor.

17.2. A büntetőjogi felelősségre vonáson túl bíróság eljárása során a Ptk. személyiségi jogok megsértésének szankcióit is alkalmazhatja.

18. Eljárási szabályok

18.1. Amennyiben a BKK Zrt. bármely szervezeti egysége, vagy szakterülete új, személyes adatokat is tartalmazó nyilvántartás vezetését határozza el, úgy erről az adatvédelmi jogszabályoknak való megfelelőséget vizsgáló konzultáció, és az adatvédelmi nyilvántartásba való bejelentés céljából köteles értesíteni a belső adatvédelmi felelőst.

18.2. A BKK Zrt.-hez érkező személyes adatokkal kapcsolatos igényeket, jogorvoslati kérelmeket haladéktalanul továbbítani kell a belső adatvédelmi felelősnek.

18.3. A belső adatvédelmi felelős a kérést kivizsgálja, amelynek eredményéről – a BKK Zrt. hatályos szabályzatainak megfelelően – értesíti a panaszos személyt, a vezérigazgatót és más érdekelteket.

18.4. A belső adatvédelmi felelős a személyes adattal kapcsolatos igények teljesítéséről, elutasításáról, annak időpontjáról és okáról nyilvántartást vezet.

18.5. A belső adatvédelmi felelős minden év nyilvántartását a következő év január 15. napjáig megküldi a Nemzeti Adatvédelmi és Információszabadság Hatóságnak.