1. számú melléklet

1/2018/1 sz. Együttes utasítás

a BKK Zrt., a BKÜ Zrt. és a BÖK Kft. együttes adatvédelmi és adatbiztonsági szabályzatáról

A BKK, BKÜ ÉS BÖK EGYÜTTES ADATVÉDELMI ÉS ADATBIZTONSÁGI SZABÁLYZATA

Dr. Hegyi Gedeon

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 Budapesti Közlekedési Központ Zártkörűen Működő Részvénytársaság (Székhely: 1075 Budapest, Rumbach Sebestyén utca 19-21., Cégjegyzékszám: 01-10-046840, továbbiakban: **BKK**), a BKÜ Budapesti Közlekedési Ügyfélkapcsolatok Zártkörűen Működő Részvénytársaság (Székhely: 1075 Budapest, Rumbach Sebestyén utca 19-21., Cégjegyzékszám: 01-10-049238, továbbiakban: **BKÜ**) és a Budapesti Önkormányzati Követeléskezelő Korlátolt Felelősségű Társaság (Székhely: 1134 Budapest, Angyalföldi út 5. B. ép., Cégjegyzékszám: 01-09-681826, továbbiakban: **BÖK**) társaságoknál 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. A BKK, a BKÜ és a BÖK együttes elnevezése a továbbiakban: **Társaságok**, külön-külön a fentiek mellett: **Társaság**. A Szabályzat kialakítja az adatvédelem szempontjából fontos feladatokat, felelősségi viszonyokat, különös tekintettel a munkavállalók szerepére az adatbiztonságban.

1.2. Jelen Szabályzat hatálya kiterjed a Társaságok székhelyén és telephelyein, valamint szolgáltatási helyszínein és eszközein folyó valamennyi személyes adat kezelésre és az üzleti titoknak minősülő adatok/információk kezelésével és védelmével kapcsolatos tevékenységekre.

1.3. A Szabályzat személyi hatálya kiterjed a Társaságok valamennyi szervezeti egységére, és munkavállalójára. A Társaságokkal szerződéses kapcsolatban álló, munkavégzésre irányuló vagy egyéb, a Szabályzat tárgyi hatálya alá tartozó tevékenységet is érintő jogviszonyban álló személyekre (így különösen adatfeldolgozókra, további-adatfeldolgozókra és olyan adatkezelőkre, amelyekkel a BKK vagy a BKÜ, vagy a BÖK közös adatkezelést folytat) a szabályzat alkalmazásának kötelezettségét az ezen személyekkel kötött szerződésben elő kell írni.

1.4. A Szabályzat tárgyi hatálya kiterjed a Társaságok szervezeti egységei által a Társaságok 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. A Szabályzat tárgyi hatálya nem terjed ki azon személyes adatokra és az azokon végzett adatkezelésekre, amelyek nem tartoznak az Európai Parlament és a Tanács (EU) 2016/679 rendeletének tárgyi hatálya alá, kivéve, ha a szóban forgó személyes adatokra és adatkezelésekre az általános adatvédelmi rendelet szabályait törvény alkalmazni rendeli.

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

2.1. Jelen Szabályzat jogszabályi alapját a következő törvények jelentik:
- Magyarország Alaptörvénye;
- Az Európai Parlament és a Tanács (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet; vagy GDPR)
- 2011. évi CXII. törvény – az információs önrendelkezési jogról és az információszabadságról (a továbbiakban: Infotv.);
- 2012. évi XLI. törvény a személyszállítási szolgáltatásokról;
- 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 Társaságok 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. *személyes adat:* azonosított vagy azonosítható természetes személyre („érintett") vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható;

3.2. *a személyes adatok különleges kategóriájába tartozó adat:* a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a természetes személyek egyedi azonosítását célzó genetikai és biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adat;

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

3.4. *adatkezelő*: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza;

3.5. *adatkezelés*: a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés továbbítás, terjesztés vagy egyéb módon

történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés;

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

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

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

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

3.10. *közös adatkezelés:* ha az adatkezelés céljait és eszközeit a Társaságok más adatkezelővel vagy adatkezelőkkel közösen határozzák meg;

3.11. *adatkezelői és adatfeldolgozói nyilvántartás:* az általános adatvédelmi rendelet 30. cikk (1) és (2) bekezdése szerint vezetett nyilvántartás;

3.12. *adatvédelmi incidens*: a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi;

3.13. *titok:* minden olyan, az egyes érintettről a Társaságok rendelkezésére álló, bizalmas, korlátozott terjesztésű vagy az arra jogosult által megfelelő módon valamilyen titokká minősített titoknak vagy más védendő, bizalmas információnak minősülő tény, információ, megoldás vagy adat, amely az érintett személyére, adataira, vagyoni helyzetére, személyi körülményeire, üzleti tevékenységére, gazdálkodására, tulajdonosi, üzleti kapcsolataira, valamint a Társaságok által kezelt követelésével függ össze;

3.14. *üzleti titok*: 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 sértené vagy veszélyeztetné, feltéve, hogy a titok megőrzésével kapcsolatban a vele jogszerűen rendelkező jogosultat felróhatóság nem terheli;

3.15. *NAIH:* Nemzeti Adatvédelmi és Információszabadság Hatóság, mint felügyeleti hatóság;

4. Az adatkezelő és az adatfeldolgozó

4.1. A közszolgáltatási feladatellátás tekintetében a szabályzat hatálya alá tartozó társaságok vonatkozásában:

Adatkezelő: BKK
Adatfeldolgozó: BKÜ és BÖK

4.2. Egyéb szolgáltatási feladatellátás tekintetében a szabályzat hatálya alá tartozó társaságok vonatkozásában:

Adatkezelő: BKK és BÖK
Adatfeldolgozó: BKÜ

4.3. Társaságok saját tevékenységükkel összefüggésben végzett adatkezeléseik – amikor a személyes adatok kezelésének céljait és eszközeit önállóan határozzák meg - tekintetében adatkezelők.

4.4. Adatkezelések
Az egyes adatkezelések részletes leírása a BKK, BKÜ és a BÖK által külön-külön vezetett adatkezelői és (amennyiben a Társaság adatfeldolgozónak minősül) adatfeldolgozói nyilvántartásban találhatóak.

II. ADATVÉDELEM

5. Adatkezelési alapelvek

5.1. Az érintettek személyes adataikhoz való jogának érvényesítése érdekében a Társaságok tiszteletben tartják az adatvédelmi jog – a fent hivatkozott jogszabályokban lefektetett – szolgáltatásaik nyújtása során alkalmazandó alapelveit, így:

5.1.1. A személyes adatokat jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kezelik (a lehetséges jogalapok tekintetében lásd az 6. pontot, az egyes adatkezelések jogalapjainak részleteire lásd a Társaságok által vezetett adatkezelői és adatfeldolgozói nyilvántartást).

5.1.2. Személyes adatokat kizárólag meghatározott, egyértelmű és jogszerű célból kezelnek (az egyes adatkezelések céljaira lásd a Társaságok által vezetett adatkezelői és adatfeldolgozói nyilvántartást).

5.1.3. Kizárólag az adatkezelés céljai szempontjából megfelelő és releváns személyes adatokat kezelnek, a szükséges mértékben (az egyes adatkezelések során kezelt személyes adatok körére lásd a Társaságok által vezetett adatkezelői és adatfeldolgozói nyilvántartást).

5.1.4. A személyes adatok pontosságát és szükség esetén naprakészségét biztosítja és minden ésszerű intézkedést megtesz annak érdekében, hogy

az adatkezelés céljai szempontjából szükségtelen személyes adatokat haladéktalanul töröljék vagy helyesbítsék.

5.1.5. A személyes adatokat olyan formában tárolja, amely az érintettek azonosítását kizárólag a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé.

5.1.6. A személyes adatokat oly módon kezeli, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelem.

5.1.7. A személyes adatok kezelését a Társaságok oly módon végzik, hogy képesek legyenek a fenti alapelveknek történő megfelelés igazolására.

5.1.8. A személyes adat védelmével kapcsolatos szabályozásra és ennek módosítására történő javaslattétel a Társaságok adatvédelmi tisztviselőinek feladata. Ha a BKK, BKÜ és a BÖK bármely munkavállalója az társaság(ok) személyes adatkezelését érintő körülményt érzékel (valamely érintett adatkezelést illető kérelme érkezik hozzá, adatvédelmi incidenst tapasztal, vagy bármely egyéb releváns információ birtokába jut), haladéktalanul köteles értesíteni a saját munkáltatójának adatvédelmi tisztviselőjét, és továbbítani neki a releváns dokumentumokat.

6. Az adatkezelés jogalapja

6.1. Személyes adatot a Társaságok kizárólag az alábbi esetekben kezelnek:

6.1.1. Ha az az érintett hozzájárulását adta személyes adatainak kezeléséhez;

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

6.1.3. Ha az adatkezelés a BKK-ra vagy BKÜ-re vagy a BÖK-re vonatkozó jogi kötelezettség teljesítéséhez szükséges;

6.1.4. Ha az adatkezelés közérdekű jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges;

6.1.5. Ha az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges;

6.1.6. Ha az adatkezelés a BKK, a BKÜ, a BÖK vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai

és szabadságai, amelyek személyes adatok védelmét teszik szükségessé, különösen, ha az érintett gyermek;

6.2. Ha az adatkezelés jogalapja a Társaság, vagy a Társaságok jogos érdeke, akkor érdekmérlegelési teszt lefolytatása szükséges. Ezen teszt keretében különösen

6.2.1. Meg kell határozni, hogy mi alkotja a BKK, a BKÜ, a BÖK vagy a harmadik fél jogos érdekét;

6.2.2. Meg kell vizsgálni, hogy mi alkotja az érintettnek olyan érdekeit, vagy alapvető jogait és szabadságait, amelyek a személyes adatok védelmét teszik szükségessé;

6.2.3. Az 6.2.1 és 6.2.2. pontban írt tényezők alapján előzetes mérlegelést kell elvégezni;

6.2.4. Az előzetes mérlegelés eredményéhez képest, amennyiben az érdekmérlegelés eredménye nem egyértelmű, további garanciákat kell társítani az érintett jogainak védelme érdekében.

6.2.5. Az elszámoltathatóság elve alapján az 6.2.1-6.2.4 pontban leírt mérlegelés elvégzését és annak eredményét dokumentálni kell.

6.2.6. Az érdekmérlegelés speciális, vagy részletesebb szabályait az Társaságok erre vonatkozó külön szabályzatban szabályozhatják.

7. A személyes adatok különleges kategóriái

7.1. A személyes adatok különleges kategóriáiba tartozó személyes adatokat a Társaságok kizárólag az érintett kifejezett, írásos hozzájárulása alapján kezelnek, kizárólag ez esetben is a hozzájárulásban meghatározott adatkezelési cél megvalósulásáig.

7.2. A 7.1. pontban meghatározott hozzájárulás hiányában az érintett által megküldött, a személyes adatok valamely különleges kategóriájába tartozó személyes adatot tartalmazó iratot a Társaságok másolat készítése nélkül visszaküldik/az elektronikus dokumentumot, tartalmat véglegesen és helyreállíthatatlanul törlik (utóbbiról értesítve az érintettet).

7.3. A 7.1. alatti hozzájárulást megfelelően dokumentálni kell.

8. Feladatok az adatkezelések során

8.1. Az adatvédelmi tisztviselő

A BKK vezérigazgatója, a BKÜ vezérigazgatója és a BÖK ügyvezetője a jelen Szabályzatban foglaltak teljesítésének felügyelete és a GDPR-ban az adatvédelmi

tisztviselői feladatok ellátása érdekében a saját Társaságánál adatvédelmi tisztviselőt nevez ki. Az adatvédelmi tisztviselő független, a feladatai ellátásával kapcsolatban senki nem utasíthatja. Az adatvédelmi tisztviselő közvetlenül a saját Társasága, azaz a BKK, vagy a BKÜ vezérigazgatójának, vagy a BÖK ügyvezetőjének tartozik felelősséggel.

Az adatvédelmi tisztviselők elérhetősége:

BKK: adatvedelem@bkk.hu

BKÜ: adatvedelem@bku.hu

BÖK: adatvedelem@bokkft.hu

Az egyes adatvédelmi tisztviselők feladatai, tevékenységei:

a) együttműködik a másik két Társaság adatvédelmi tisztviselőjével, valamint azon adatkezelések tekintetében, amelyeknél valamely Társaság adatfeldolgozási tevékenységet lát el, folyamatos kapcsolatot tart a másik érintett Társaság adatvédelmi tisztviselőjével;

b) tájékoztat és szakmai tanácsot ad a saját munkáltatója/megbízója, továbbá a saját Társasága adatkezelést végző alkalmazottainak részére az általános adatvédelmi rendelet, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezések szerinti kötelezettségeikkel kapcsolatban;

c) ellenőrzi az általános adatvédelmi rendeletnek, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezéseknek, továbbá jelen szabályzatnak és a munkáltatójának/megbízójának egyéb, személyes adatkezelést illető szabályzatainak való megfelelést, ideértve a feladatkörök kijelölését, az adatkezelési műveletekben vevő személyzet tudatosság-növelését és képzését, valamint a kapcsolódó auditokat is;

d) kérésre szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, valamint nyomon követi a hatásvizsgálatnak az általános adatvédelmi rendelet 35. cikke szerinti elvégzését;

e) együttműködik a Nemzeti Adatvédelmi és Információszabadság Hatósággal;

f) az adatkezeléssel összefüggő ügyekben – ideértve az általános adatvédelmi rendelet 36. cikkben említett előzetes konzultációt is – kapcsolattartó pontként szolgál a NAIH, valamint adott esetben bármely egyéb kérdésben konzultációt folytat vele.

8.2. A szervezeti egységek vezetői

a) felelősek az irányításuk alá tartozó szervezeti egységek adatkezelései vonatkozásában a jogszabályoknak és jelen Szabályzatnak való megfelelőségéért,

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

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

d) a személyes adatkezeléssel vagy adatfeldolgozással kapcsolatos tervezett tevékenységeket bejelentik az adatvédelmi tisztviselőnek.

8.3. Az adatkezelést végző személy

A Társaságok 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,

f) az Incidenskezelési Rendnek megfelelően eljárva értesíti a kijelölt személyeket incidens gyanúja esetén.

9. Az érintetti jogok gyakorlása

9.1. Az érintettek jogaikat kérelemre gyakorolhatják.

9.2. A Társaságok a kérelem beérkezésétől számított egy hónapon tájékoztatni kötelesek az érintettet a kérelemre adott válaszról, amely határidő szükség esetén - a kérelem összetettségére és a kérelmek számára tekintettel - további két hónappal meghosszabbítható. A határidő meghosszabbításáról a kérelem beérkezésétől számított egy hónapon belül kell tájékoztatni az érintettet a késedelem okainak megjelölésével. Ha az érintett elektronikus úton nyújtotta be a kérelmet, a tájékoztatást is elektronikus úton kell megadni, kivéve, ha az érintett azt másként kéri, mindenkor tekintetbe véve ugyanakkor a titok megőrzésére vonatkozó szabályokat is.

9.3. A Társaságokhoz való beérkezésnek az az időpont számít, amikor az érintett kérelme az adott Társasághoz hiánytalanul és hiteles módon beérkezik. Amennyiben a kérelemmel érintett Társaság úgy érzékeli, hogy a kérelem tartalma nem egyértelmű vagy hiányos, további pontosítást kérhet az érintettől és ebben az esetben az ügyintézési határidő csak a hiánypótlás, illetve pontosítás beérkezését követően kezdődik.

9.4. A kérelemben foglaltak teljesítését a Társaságok a következő esetekben jogosultak megtagadni:

- az érintett nem a saját adataira vonatkozóan terjeszt elő kérelmet és nem rendelkezik érvényes meghatalmazással az adatok megismerésére;

- a kérelmet előterjesztő személy nem tudja vagy nem hajlandó hitelt érdemlő módon igazolni, hogy ő az adatkezeléssel érintett személy, illetve annak meghatalmazottja;
- az adott Társaság az adatokat egy másik adatkezelőtől akként vette át, hogy az adatokat átadó adatkezelő jelezte, hogy az érintett kérelmezési joga korlátozott és ezen korlátozás a magyar jog szerint is érvényesülhet;
- az érintett a költségtérítés összegét nem hajlandó megfizetni;
- ha az adott Társaság megítélése szerint kérelem egyértelműen megalapozatlan (így például az érintett már rendelkezik a kért információkkal, hisz előzetes tájékoztatás keretében már megkapta azokat vagy azok számára hozzáférhetők) vagy túlzó;
- a kérelemben foglaltak teljesítését jogszabály zárja ki.

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

9.6. Az érintett jogaival kapcsolatos és az adatvédelmi incidensről szóló tájékoztatást és intézkedést díjmentesen kell biztosítani. Ha az érintett kérelme egyértelműen megalapozatlan vagy - különösen ismétlődő jellege miatt - túlzó, a Társaságok, figyelemmel a kért információ vagy tájékoztatás nyújtásával vagy a kért intézkedés meghozatalával járó adminisztratív költségekre, díjat számíthatnak fel, vagy megtagadhatják a kérelem alapján történő intézkedést.

9.7. A kérelem egyértelműen megalapozatlan vagy túlzó jellegének bizonyítása az adott, kérelemmel érintet Társaságot terheli.

10. A közreműködő személyekre vonatkozó különös rendelkezések

10.1. A közreműködő személyek adatainak felvétele és felhasználása

A közreműködő személyek személyes adatait a Társaságok csak kivételes esetekben, illetve kizárólag az ügyféllel megkötendő szerződések teljesítésével összefüggésben, az érintett közreműködő személyek kifejezett hozzájárulása alapján kezelik, vagy vélelmezik, hogy az ügyfelek rendelkeznek ezen adatok jogszerű felhasználására felhatalmazással az általuk kezdeményezett eljárások során.

A hozzájárulások meglétét és jogszerűségét az ügyféllel megkötendő szerződések, illetve az ügyféllel kapcsolatos követeléskezelési tevékenység esetén a Társaságok vélelmezik – azok jogszerűségéért az ügyfél tartozik felelősséggel –, ugyanakkor a Társaságok fenntartják maguknak a jogot, hogy ezen érintetti hozzájárulások valóságtartalmát ellenőrizzék és szükség esetén ezen érintetteket közvetlenül megkeressék hozzájárulásuk meglétének ellenőrzése, vagy hozzájárulásuk megszerzése érdekében.

A Társaságok alapvetően a következő adatokat kezelik ezen érintettekről:

- személyazonosító adataikat;

- kapcsolati, elérhetőségi adataikat;
- az ügyféllel fennálló kapcsolatukra vonatkozó adataikat;
- vagyoni-, tulajdoni adataikat;
- az ügyféllel megkötendő szerződések vagy az ügyfelet érintő követelés teljesítéséhez szükséges nyilatkozataikat, illetve kötelezettségvállalásaikat.

A Társaságok ezen adatokat az ügyféllel megkötendő szerződéssel együtt kezelik, annak teljesülését, illetve megszűnését követő 8. év elteltével – kivéve, ha jogszabály ettől eltérő megőrzési időt ír elő – az adatokat lehetőség szerint törlik vagy anonimizálják.

A Társaságok e körben is jogosultak – az ügyfélre vonatkozó adatokhoz kapcsoltan – ezen egyéb érintetti adatokat is továbbítani az adott Társaság közvetett tulajdonosa, illetve végső soron a Fővárosi Önkormányzat, mint a Társaságok végső tulajdonosa felé, az ügyfelekre irányadó szabályok szerint és célokból.

10.2. A közreműködő személyeket megillető jogok

A közreműködő személyeket az ügyfélhez hasonló adatvédelmi jogok illetik meg, gyakorlásukra az ügyfelekre irányadó szabályok érvényesek. (Ezen személyek csak a saját adataik kapcsán fordulhat kérelemmel, illetve panasszal a kérelemmel érintett Társasághoz).

Az adott kérelemmel érintett Társaság ezen kérelem, illetve panasz teljesítését ugyanakkor jogosult abban az esetben is elutasítani, ha a teljesítéssel titkot vagy az ügyfél jogait sértené.

Amellett, hogy erre az ügyfél köteles, a közreműködő személy önállóan is jogosult arra, hogy a Társaságok által kezelt személyes adataiban beállt változásokról haladéktalanul, de legkésőbb 5 munkanapon belül értesítse az adott Társaságot és a személyes adatok módosítását, helyesbítését kérje.

11. Az érintett tájékoztatáshoz fűződő joga

11.1. A BKK és a BKÜ elsősorban az érintettektől jut személyes adataik birtokába. Ha a személyes adatokat nem az érintettől szerzi be, a BKK, BKÜ a következő információkat bocsátja az érintett rendelkezésére:

11.1.1. a BKK, BÖK (amennyiben az adatkezeléssel kapcsolatban szükséges), illetőleg a BKÜ és képviselőjüknek a kiléte és elérhetőségei;

11.1.2. a BKK, BÖK (amennyiben az adatkezeléssel kapcsolatban szükséges), illetőleg a BKÜ adatvédelmi tisztviselőjének elérhetőségei;

11.1.3. a személyes adatok tervezett kezelésének célja, valamint az adatkezelés jogalapja;

11.1.4. az érintett személyes adatok kategóriái;

11.1.5. a személyes adatok címzettjei, illetve a címzettek kategóriái; ha van ilyen, a személyes adatok harmadik országokba történő továbbítása esetén az Általános Adatvédelmi Rendeletben meghatározott információk;

11.1.6. a személyes adatok tárolásának időtartama, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjai;

11.1.7. ha az adatkezelés jogalapja a Társaság, vagy a Társaságok jogos érdeke, akkor mely érdek a BKK, BÖK, illetőleg a BKÜ jogos érdeke;

11.1.8. Az a tény, hogy az érintett kérelmezheti az adatkezelőtől a rá vonatkozó személyes adatokhoz való hozzáférést, azok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat a személyes adatok kezelése ellen, valamint az érintett élhet adathordozhatósághoz való jogával;

11.1.9. Hozzájáruláson alapuló adatkezelés esetén a hozzájárulás bármely időpontban való visszavonásához való jog, amely nem érinti a visszavonás előtt a hozzájárulás alapján végrehajtott adatkezelés jogszerűségét;

11.1.10. A NAIH-hoz mint felügyeleti hatósághoz címzett panasz benyújtásának joga;

11.1.11. A személyes adatok forrása és adott esetben az, hogy az adatok nyilvánosan hozzáférhető forrásokból származnak-e;

11.1.12. Automatizált döntéshozatal ténye, ideértve a profilalkotást is, valamint legalább ezekben az esetekben az alkalmazott logikára és arra vonatkozó érthető információk, hogy az ilyen adatkezelés milyen jelentőséggel, és az érintettre nézve milyen várható következményekkel bír;

11.2. A tájékoztatási jog keretében az információkat a személyes adatok kezelésének konkrét körülményeit tekintetbe véve, a személyes adatok megszerzésétől számított ésszerű határidőn, de legkésőbb egy hónapon belül kell közölni, mely határidő szükség esetén, figyelembe véve a kérelem összetettségét és a kérelmek számát, további két hónappal meghosszabbítható. A határidő meghosszabbításáról a késedelem okainak megjelölésével a kérelem kézhezvételétől számított egy hónapon belül tájékoztatni szükséges az érintettet. Amennyiben a személyes adatokat az érintettel való kapcsolattartás céljára használják, legalább az érintettel való első kapcsolatfelvétel alkalmával kell közölni az információkat.

11.3. A tájékoztatás jogának gyakorlása csak az általános adatvédelmi rendelet 14. cikk (5) bekezdésében foglalt esetekben tagadható meg.

12. Az érintett hozzáférési joga

12.1. A BKK, BKÜ és a BÖK az érintett igényére visszajelzést ad arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e, és ha ilyen adatkezelés folyamatban van, hozzáférést biztosít a személyes adatokhoz és a következő információkhoz:

12.1.1 az adatkezelés céljai;

12.1.2. az érintett személyes adatok kategóriái;

12.1.3. azon címzettek vagy címzettek kategóriái, akikkel, illetve amelyekkel a személyes adatokat közölték vagy közölni fogják, ideértve különösen a harmadik országbeli címzetteket;

12.1.4. adott esetben a személyes adatok tárolásának tervezett időtartama, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjai;

12.1.5. az érintett azon joga, hogy kérelmezheti az adatkezelőtől a rá vonatkozó személyes adatok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen;

12.1.6. a valamely felügyeleti hatósághoz címzett panasz benyújtásának joga;

12.1.7. ha az adatokat nem az érintettől gyűjtötték, a forrásukra vonatkozó minden elérhető információ;

12.1.8 az automatizált döntéshozatal ténye, ideértve a profilalkotást is, valamint legalább ezekben az esetekben az alkalmazott logikára és arra vonatkozó érthető információk, hogy az ilyen adatkezelés milyen jelentőséggel bír, és az érintettre nézve milyen várható következményekkel jár.

12.1.9 ha személyes adatoknak harmadik országba történő továbbítására kerül sor, az érintett jogosult arra, hogy tájékoztatást kapjon a továbbításra vonatkozó garanciákról.

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

13. A helyesbítéshez és törléshez való jog

13.1. Az érintett kérésére a BKK, BKÜ illetőleg a BÖK indokolatlan késedelem nélkül helyesbíti a rá vonatkozó pontatlan személyes adatokat, valamint - figyelembe véve az adatkezelés célját - az érintett erre irányuló kérése esetén biztosítja a hiányos személyes adatok – egyebek mellett kiegészítő nyilatkozat útján történő – kiegészítését.

13.2. A BKK, BKÜ, illetőleg a BÖK az érintett kérésére indokolatlan késedelem nélkül törli a rá vonatkozó személyes adatokat, ha

13.2.1. a személyes adatokra már nincs szükség abból a célból, amelyből azokat gyűjtötték vagy más módon kezelték;

13.2.2. az érintett visszavonja az adatkezelés alapját képező hozzájárulását, és az adatkezelésnek nincs más törvényes jogalapja;

13.2.3. az érintett tiltakozik az adatkezelése ellen, és nincs elsőbbséget élvező jogszerű ok az adatkezelésre, vagy az adatainak direktmarketing célú felhasználása ellen tiltakozik;

13.2.4. az érintett személyes adatainak kezelése jogszerűtlen;

13.2.5. a személyes adatokat a BKK-ra, BKÜ-re, illetve a BÖK-re alkalmazandó uniós vagy tagállami jogban előírt jogi kötelezettség teljesítése okán törölni kell;

13.2.6. a személyes adatok gyűjtésére gyermekek számára nyújtott információs társadalommal összefüggő szolgáltatások nyújtásával kapcsolatban került sor.

13.2.7. Az érintetti jogok korlátozására kizárólag az általános adatvédelmi rendeletben írt kivételek fennállása esetén kerülhet sor.

13.3. A BKK, BKÜ, illetőleg a BÖK minden olyan címzettet tájékoztat valamennyi helyesbítésről vagy törlésről akivel, illetve amellyel a személyes adatot közölték, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel. Az érintettet kérésére a BKK, BKÜ, illetőleg a BÖK tájékoztatja e címzettekről.

14. Személyes adat kezelésének korlátozásához való jog

14.1. Az érintett kérelmére a BKK, BKÜ, illetőleg a BÖK korlátozza az adatkezelést, ha

14.1.1. az érintett vitatja a személyes adatok pontosságát, ez esetben a korlátozás arra az időtartamra vonatkozik, amely lehetővé teszi, hogy az adatkezelő ellenőrizze a személyes adatok pontosságát

14.1.2. az adatkezelés jogellenes, és az érintett ellenzi az adatok törlését, és ehelyett kéri azok felhasználásának korlátozását

14.1.3. az adatkezelőnek már nincs szüksége a személyes adatokra adatkezelés céljából, de az érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez;

14.1.4. az érintett jogos érdeken vagy közérdekű célból végzett adatkezelés ellen tiltakozott; ez esetben a korlátozás arra az időtartamra vonatkozik, amíg megállapításra nem kerül, hogy az adatkezelő jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben.

14.2. A BKK, BKÜ, illetőleg a BÖK minden olyan címzettet tájékoztat valamennyi adatkezelést illető korlátozásról, akivel, illetve amellyel a személyes adatot közölték, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel. Az érintettet kérésére a BKK, BKÜ, illetőleg a BÖK tájékoztatja e címzettekről.

15. Az adathordozhatósághoz való jog

15.1. Az érintett jogosult arra, hogy a rá vonatkozó, a BKK, BKÜ, illetőleg a BÖK rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja, továbbá jogosult arra, hogy ezeket az adatokat egy másik adatkezelőnek továbbítsa, ha

15.1.1. az adatkezelés az általános adatvédelmi rendelet szerinti hozzájáruláson vagy szerződésen, mint jogalapon alapszik vagy

15.1.2. az adatkezelés automatizált módon történik.

15.2. Az adathordozhatósághoz való jog alkalmazásának kizárására és korlátozására az általános adatvédelmi rendelet szabályait kell alkalmazni.

16. A tiltakozáshoz való jog

16.1. Az érintett bármikor tiltakozhat a saját helyzetével kapcsolatos okokból a közérdekű célból vagy jogos érdekből végzett adatkezelés ellen, ideértve a profilalkotást is. Ebben az esetben a BKK, BKÜ, illetőleg a BÖK a személyes adatokat nem kezelheti tovább, kivéve, ha bizonyítja, hogy az adatkezelést olyan okok indokolják, amelyek elsőbbséget élveznek az érintett érdekeivel, jogaival és szabadságaival szemben, vagy amelyek jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódnak.

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

17. Automatizált döntéshozatal, profilalkotás

17.1. A BKK, BKÜ, illetőleg a BÖK csak akkor alkalmaz kizárólag automatizált adatkezelésen – ideértve a profilalkotást is – alapuló döntést, amely az érintette nézve joghatással jár vagy őt hasonlóképpen jelentős mértékben érinti, ha

17.1.1. a BKK, BKÜ, illetőleg a BÖK és az érintett közötti szerződés megkötése vagy teljesítése érdekében szükséges;

17.1.2. meghozatalát a BKK-ra, BKÜ-re illetőleg a BÖK-re alkalmazandó olyan uniós vagy hazai jogszabály teszi lehetővé, amely az érintett jogainak és szabadságainak, valamint jogos érdekeinek védelmét szolgáló megfelelő intézkedéseket is megállapít

17.1.3. az érintett kifejezett hozzájárulásán alapul.

17.2. Az automatizált döntés és profilalkotás további követelményeire az általános adatvédelmi rendelet alkalmazandó.

18. Incidenskezelés adatkezelőként

18.1. Az adatvédelmi incidenst a BKK, BKÜ, illetőleg a BÖK a tudomására jutását követően indokolatlan késedelem nélkül, ha lehetséges, legkésőbb 72 órán belül bejelenti a Nemzeti Adatvédelmi és Információszabadság Hatóságnak. A bejelentést a NAIH által megadott formában és módon kell megtenni, a hatóság előírásai szerint (például a hatóság által megjelölt felületen).

18.2. Ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve, a bejelentést nem kell megtenni. Ezt a döntést a BKK vezérigazgatója, a BKÜ vezérigazgatója és a BÖK ügyvezetője hozza meg a saját Társasága vonatkozásában, mérlegelve az eset összes körülményeit, az adatvédelmi tisztviselővel történő konzultációt követően.

18.3. A BKK, BKÜ, illetőleg a BÖK nyilvántartja az adatvédelmi incidenseket, feltüntetve az adatvédelmi incidenshez kapcsolódó tényeket, annak hatásait és az orvoslására tett intézkedéseket. Az incidensek nyilvántartására legalább a felügyeleti hatóság (NAIH) által meghatározott kötelező tartalmi elemeket tartalmazó incidens nyilvántartási táblázatot kell alkalmazni.

18.4. A BKK, BKÜ, illetőleg a BÖK indokolatlan késedelem nélkül tájékoztatja az érintettet az adatvédelmi incidensről, ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve. Ezt a döntést A BKK vezérigazgatója, a BKÜ vezérigazgatója és a BÖK ügyvezetője hozza meg a saját Társasága vonatkozásában az eset összes körülményeire tekintettel, az adatvédelmi tisztviselővel való konzultációt követően. A döntésről az adatvédelmi tisztviselő feljegyzést készít.

18.5. Az érintett értesítése alóli kivétel, ha

18.5.1. A BKK, BKÜ, illetőleg a BÖK megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre, és ezeket az intézkedéseket az adatvédelmi incidens által érintett adatok tekintetében alkalmazta, különösen azokat az intézkedéseket – mint például a titkosítás alkalmazása –, amelyek a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik az adatokat; vagy

18.5.2. A BKK, BKÜ, illetőleg a BÖK az adatvédelmi incidenst követően olyan további intézkedéseket tett, amelyek biztosítják, hogy az érintett jogaira és szabadságaira jelentett magas kockázat a továbbiakban valószínűsíthetően nem valósul meg; vagy

18.5.3. Az egyedi tájékoztatás aránytalan erőfeszítést tenne szükségessé, így ehelyett az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, vagy olyan hasonló intézkedést kell hozni, amely biztosítja az érintettek hasonlóan hatékony tájékoztatását.

18.6. Az adatkezelőként történő indicenskezelésére vonatkozó folyamat leírását a BKK, BKÜ, illetőleg a BÖK közös Incidenskezelési Rendje tartalmazza, mely jelen szabályzat mellékletét képezi.

19. Közös adatkezelés

19.1. Közös adatkezelés esetén az adatkezelők a közöttük létrejött megállapodásban határozzák meg az általános adatvédelmi rendeletben foglalt kötelezettségek teljesítéséért fennálló felelősségük megoszlását, különösen az érintettek jogainak gyakorlásával és tájékoztatásával kapcsolatban. A megállapodásban a BKK, BKÜ, illetőleg a BÖK és a további adatkezelők az érintettek számára kapcsolattartót jelölnek ki.

19.2. A fenti pontban hivatkozott megállapodás lényegét az érintett rendelkezésére kell bocsátani.

19.3. Az érintett jogait abban az esetben is biztosítani kell, ha az a fenti pontban hivatkozott megállapodástól eltérően kívánja azokat gyakorolni.

20. Adatfeldolgozó igénybevétele

20.1. A BKK, BKÜ, illetőleg a BÖK adatkezelőként csak olyan adatfeldolgozókat vesz igénybe, amelyek megfelelnek az általános adatvédelmi rendelet előírásainak. Az adatfeldolgozási szerződést írásban kell megkötni, és annak eleget kell tennie az e pontban szabályozott tartalmi követelményeknek.

20.2. Az adatfeldolgozási szerződésben rendelkezni kell arról, hogy az adatfeldolgozó további adatfeldolgozót nem vehet igénybe, vagy általános felhatalmazást vagy

egyedi felhatalmazás lehetőségét kell rögzíteni további adatfeldolgozó igénybevételére. Ha az adatfeldolgozó bizonyos, a BKK, BKÜ, illetőleg a BÖK nevében végzett konkrét adatkezelési tevékenységekhez további adatfeldolgozó szolgáltatásait is igénybe veszi létrehozandó szerződésben, erre a további adatfeldolgozóra is ugyanazok az adatvédelmi kötelezettségeket kell telepíteni, mint amelyek a BKK, BKÜ, illetőleg a BÖK és az adatfeldolgozó között létrejött szerződésben szerepelnek.

20.3. Az adatfeldolgozási szerződésben rögzíteni kell, hogy az adatfeldolgozó a személyes adatokat kizárólag a BKK, BKÜ, illetőleg a BÖK írásbeli utasításai alapján kezel, és rendelkezni szükséges az adatfeldolgozási szerződésben, valamennyi, adatvédelmi rendelet által előírt követelményről.

21. A BKK, BKÜ és a BÖK mint adatfeldolgozó

21.1. Ha a BKK, BKÜ, illetőleg a BÖK adatfeldolgozóként jár el, a szolgáltatás kapcsán végzett személyes adatkezelések jogalapjának meghatározása és jogszerűségének biztosítása a megbízó, mint adatkezelő kötelezettsége. A megbízó felel azon adatkezelések jogszerűségéért, amelyek végrehajtásához a BKK-t, BÖK-öt, illetőleg a BKÜ-t igénybe veszi. A BKK, BKÜ illetőleg a BÖK a szerződésben meghatározott intézkedésekkel segíti az adatkezelőt az adatvédelmi szabályozásnak való megfelelésben.

21.2. Az adatkezelővel a BKK, BKÜ, illetőleg a BÖK írásbeli adatfeldolgozási szerződést köt. Az adatfeldolgozási szerződést úgy kell megkötni, hogy az tartalmazza a GDPR-ban, illetve a jelen Szabályzatban az adatfeldolgozási szerződésre előírt tartalmi elemeket.

22. Az adatok felhasználása és továbbítása

22.1. A Társaságok az érintettek adatait lehetőségei szerint saját, illetve befolyásuk alatt álló szervezetek rendszereiben tárolják, de mindenkor lehetőségük van harmadik személynek tekintendő adatfeldolgozó vagy adatkezelő megbízására is. Függetlenül azonban a tárolás helyétől és az azt végző személyétől és módjától, minden adattárolás úgy történik, hogy a tárolt adatokhoz illetéktelenek – ideértve a Társaságok azon munkavállalóit és a Társaságokkal/valamely Társasággal szerződéses vagy egyéb kapcsolatban álló adatkezelési vagy adatfeldolgozási tevékenységet végző személyeket is, akik nem jogosultak ezen adatok megismerésére, kezelésére – ne férhessenek hozzá, az adatok bizalmassága ne sérülhessen, biztosított maradjon az adat teljes életciklusa alatt.

22.2. A Társaságok az érintettek személyes adatait kizárólag a megkötött szerződésekben, valamint a tevékenységükre irányadó jogszabályokban, továbbá az adatfelvételkor meghatározott célból – illetve adatátvétel esetén, az ott jelzett célból – használják fel a jelen Szabályzatban foglalt keretek között.

22.3. Amennyiben a Társaságok bármilyen más célra is fel kívánnák használni az érintettek adatait, arra csak a következő módokon kerülhet sor:

- az új célú felhasználást jogszabályváltozás vagy a jogszabályoknak való megfelelés szükségessége idézi elő – ennek bekövetkeztéről, az előállt változásokról a Társaságok az Általános Üzleti Feltételeiben beállt változásoknak megfelelő módon, elsősorban hirdetményben, illetve honlapján keresztül vagy email-ben értesítik ügyfeleiket;

- a felhasználási cél változása a Társaságok érdekkörében merül fel, úgy ennek bekövetkeztéről – amennyiben ez lehetséges és szükséges – a Társaságok külön értesítik ügyfeleiket (az előbbi módokon) és egyúttal, ha ez szükséges, hozzájárulásukat kéri adataik ezen új cél szerinti felhasználásához;

- adatátvétel esetén, ha az új célú felhasználást az adatátvételkor nem zárták ki, akkor az eredeti adatkezelő egyidejű értesítésével, egyebekben kizárólag előzetes hozzájárulással;

- az adatok személyes jellegétől való megfosztása (ún. anonimizálása) révén.

22.4. A Társaságok és ügyfeleik közötti szerződéses kapcsolatok esetén megvalósuló, illetve egyéb adatkezelési célokhoz igazodó konkrét felhasználási tevékenységeket elsődlegesen az adott Társaság által alkalmazott Adatkezelési Tájékoztató, illetve kiegészítő jelleggel, az ügyféllel megkötött konkrét szerződések, továbbá a mindezekhez kapcsolódó nyilatkozatok és tájékoztatók tartalmazzák.

23. Adattovábbítás és hatósági adatszolgáltatás

23.1. Az adattovábbítások általános szabályai

23.1.1. A Társaságok a kezelésükben lévő adatokat, ha azt jogszabály kötelezővé teszi, vagy ha az a szerződés teljesítése érdekében szükség van, vagy ha ez jogos érdekre tekintettel lehetséges, vagy ha az érintett ügyfél hozzájárulása (ideértve az ügyfél által adott szabályos meghatalmazást is) lehetővé teszi, jogosult, illetve köteles az arra jogosult számára továbbítani vagy hozzáférhetővé tenni;

23.1.2. Az adatok továbbítására a titkokra vonatkozó rendelkezések is megfelelően alkalmazandók a jelen Szabályzat rendelkezései mellett.

23.1.3. Amennyiben nem egyértelmű, hogy az érintett adatok továbbíthatóak-e, úgy az adatátadást megelőzően az adatvédelmi tisztviselőhöz kell fordulni, aki véleményt ad az adattovábbítás megengedhetősége kérdésében. Az adatvédelmi tisztviselő megkeresésének elmulasztása esetén az adatátadás esetleges jogszerűtlenségéért a felelősség kizárólag az adatkezelésért felelős terület vezetőjét terheli.

23.1.4. A Társaságok az ügyfeleikről tudomására jutott titkokat, illetve személyes adatokat továbbíthatják az adatkezelés céljához igazodóan az ügyfél hozzájárulásával, vagy ha az a szerződés teljesítéséhez szükséges, vagy amennyiben arra Társaságok számára jogszabály kötelezettséget ró, vagy az adott Társaság vagy más harmadik fél jogos érdekére tekintettel – többek között különösen a következő esetekben:

- hatályos adatfeldolgozói szerződés, további adatkezelő igénybevétele vagy társ-adatkezelő adatfeldolgozó általi bevonása esetén, a jelen Szabályzatban az adatkezelés lehetséges céljainál meghatározott okokból;

- egy további adatkezelővel megkötött közös adatkezelési szerződés teljesítése érdekében;

- az ügyféllel megkötött szerződés teljesítése vagy a szerződéssel összefüggésben vállalt kötelezettségek teljesítése, illetve ezek ellenőrzése érdekében;

- statisztikai adatszolgáltatási kötelezettség teljesítése érdekében;

- követelés kezelése, illetve értékesítése keretében az adott Társaság átadhatja az ügyfél adatait, ha azok az adott Társaságnak az ügyféllel szemben fennálló követelése eladásához vagy késedelmes, lejárt követelése érvényesítéséhez szükségesek, az adott Társaság az adatokat olyan harmadik személy részére adhatja át, akinek vonatkozásában az a követelés eladásához vagy érvényesítéséhez

szükséges, így különösen annak, akire az adott Társaság az ügyféllel szembeni követelését átruházza vagy amelyet ezen követelés kezelésével megbíz;

- hatósági, illetve bírósági adatszolgáltatási kötelezettség teljesítése érdekében;

- az adott Társaság tulajdonosa részére, illetve a leányvállalatok és érdekeltségek közötti adatáramlás biztosítása érdekében – e felek között megkötött adatátadási szerződések keretei között, amennyiben az szükséges, úgy az ügyfél hozzájárulásával.

23.2. Hatósági adatszolgáltatások

23.2.1. Az adatkérésre jogszabály alapján jogosult nyomozó hatóság, ügyészség, bíróság, nemzetbiztonsági szolgálat, minősített adatok kezelésére jogosult, vagy ilyen megkeresés küldésére jogosult szerv vagy más hatóság (például jegyző, közjegyző, GVH, adóhatóság, Államkincstár, alapvető jogok biztosa, NAIH, stb.) törvényben meghatározott feladatai ellátásának biztosítása céljából elrendelt vagy kérelmezett adatszolgáltatási igényének a Társaságok eleget tesznek, ezen szervek, szervezetek felé titoktartási kötelezettsége a vonatkozó jogszabályi keretek között a Társaságoknak a saját ügyfeleik vonatkozásában nem áll fenn, így e körben személyes adatokat is továbbít(hat) az érintettekről ezen szervek, szervezetek felé.

23.2.2. A szolgáltatandó adatok körét és fajtáit, a hatóság általi adatkezelés célját és feltételeit, az adatok megismerhetőségét, az azokhoz való hozzáférést, az adatkezelés időtartamát, az adattovábbításról való ügyféli értesítés lehetőségét, illetve az adatszolgáltatás teljesítésére az adott Társaság számára rendelkezésre álló időtartamot, valamint az adattovábbítás módját a vonatkozó jogszabályi keretek között az adatkezelést elrendelő szerv vagy szervezet határozza és állapítja meg.

23.2.3. Az adatátadás jogszerűségéért minden esetben az eljáró, adatszolgáltató szerv a felelős.

23.2.4. A hatósági adatszolgáltatások teljesítéséből származó esetleges ügyféligényekkel, ügyfélkárokkal kapcsolatos felelősségét a Társaságok egymás irányában kizárják.

23.2.5. Hatósági megkeresés lehet rendszeres vagy rendkívüli/eseti jellegű is.

23.2.6. A rendszeres adatszolgáltatások teljesítésére a Társaságok szervezetükön belül kijelölik az ezen adatszolgáltatások teljesítéséért felelős területeket. A rendkívüli adatszolgáltatás teljesítéséért az esetileg kijelölt szervezeti egység felelős a vonatkozó belső szabályzat keretei és eljárásrendszer szerint.

23.2.7. Az adattovábbításokról az adattovábbítás jogszerűségének ellenőrzése, valamint az érintettek tájékoztatása céljából a Társaságok saját nyilvántartást vezetnek. Ez a nyilvántartás tartalmazza az adattovábbítás jogalapját és címzettjét, a továbbított személyes adatok körének meghatározását, valamint a GDPR-ban meghatározott egyéb adatokat.

24. Adattovábbítás harmadik országba

24.1. A Társaságok személyes adatokat harmadik országba akkor továbbíthatnak, ha:

- adott ország kapcsán az Európai Bizottság megállapította, hogy a harmadik ország, a harmadik ország valamely területe, vagy egy, vagy több meghatározott ágazata, vagy az adott adatfeldolgozó, illetve a további-adatkezelő megfelelő védelmi szintet biztosít;

- az adattovábbítás címzettje megfelelő garanciákat nyújtott az adatkezelést érintően a megbízó Társaság számára, és kifejezetten biztosított, hogy az érintettek adatvédelmi jogaikat hatékonyan, megfelelő jogorvoslati lehetőségeken keresztül érvényesíteni tudják;

- jogszabály vagy nemzetközi szerződés vagy a felügyeleti hatóság külön engedélye ezt lehetővé teszi;

- az adattovábbítások kötelező erejű vállalati szabályok keretei között valósulnak meg;

- az érintett kifejezetten hozzájárulását adta a tervezett személyes adat továbbításhoz azt követően, hogy az adott, adatkezelést tervező Társaság tájékoztatta az adattovábbításból eredő – a megfelelőségi határozat és a megfelelő garanciák hiányából fakadó – esetleges kockázatokról;

- az adattovábbításra az érintett és a Társaságok/Társaság közötti szerződés teljesítéséhez, vagy az érintett kérésére hozott, szerződést megelőző intézkedések végrehajtásához van szükség;

- az adattovábbítás az adott Társaság és valamely más természetes vagy jogi személy közötti, az érintett érdekét szolgáló szerződés megkötéséhez vagy teljesítéséhez szükséges;

- az adattovábbítás jogi igények előterjesztése, érvényesítése és védelme miatt szükséges.

24.2. Harmadik országba történő adattovábbításra akkor is lehetősége van a Társaságoknak, ha a továbbított adatok olyan nyilvántartásból származnak, amely jogszabályi értelmében a nyilvánosság tájékoztatását szolgálják, és amelyek vagy általában a nyilvánosság, vagy az ezzel kapcsolatos jogos érdekét igazoló bármely személy számára betekintés céljából hozzáférhetőek, de csak ha a jogszabály által a betekintésre megállapított feltételek az adott különleges esetben teljesülnek. Ilyen

esetben az adattovábbítás nem érintheti a nyilvántartásban szereplő személyes adatok vagy személyes adatok kategóriáinak összességét. Ha a nyilvántartásba kizárólag olyan személyek tekinthetnek be, akiknek ehhez jogos érdeke fűződik, az adattovábbításra kizárólag e személyek kérelmére kerülhet sor, illetve abban az esetben, ha ők a címzettek. Mindezek hiányában kivételesen lehetséges az adattovábbítás akkor is, ha az adattovábbítás nem ismétlődő, csak korlátozott számú érintettre vonatkozik, az adott Társaság olyan kényszerítő erejű jogos érdekében szükséges, amely érdekhez képest nem élveznek elsőbbséget az érintett érdekei és jogai, és az adott Társaság az adattovábbítás minden körülményét megvizsgálta, és e vizsgálat alapján megfelelő garanciákat nyújtott a személyes adatok védelme tekintetében. A Társaságok az ilyen kivételes adattovábbításokról kötelesek a felügyeleti hatóságot és az érintettet is tájékoztatni, illetve kötelesek az adattovábbítást és a hozzá kapcsolódó megfelelőségi garanciális vizsgálat eredményeit az adatvédelmi nyilvántartásban feltűntetni.

24.3. A harmadik országba történő adattovábbításról a Társaságok önmaguk vonatkozásában ún. Adattovábbítási Nyilvántartást vezetnek. A Nyilvántartást az érintett szakterület adatszolgáltatása alapján az adott Társaság DPO-ja vezeti. A Nyilvántartásba történő adatszolgáltatás rendjére (ideértve a változás bejelentési kötelezettséget is), az előzetes felmérésre, a DPO-val való kapcsolatra és az adatszolgáltatásért való felelősségre, a NAIH részére történő információszolgáltatásra a Szabályzatban és a GDPR-ban foglaltak megfelelően irányadók.

24.4. Személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására alapértelmezetten akkor kerülhet sor, ha a Bizottság határozatban megállapította, hogy a harmadik ország, a harmadik ország valamely területe, vagy egy vagy több meghatározott ágazata, vagy a szóban forgó nemzetközi szervezet megfelelő védelmi szintet biztosít. Az ilyen adattovábbításhoz nem szükséges külön engedély. A Bizottság az olyan harmadik országok, harmadik országon belüli területek és meghatározott ágazatok, valamint nemzetközi szervezetek jegyzékét, amelyek esetében úgy ítélte meg, hogy biztosítják, vagy többé nem biztosítják a megfelelő védelmi szintet az Európai Unió Hivatalos Lapjában és annak honlapján teszi közzé.

24.5. Megfelelősségi határozat hiányában akkor kerülhet sor a személyes adat továbbításra, ha adott ország megfelelő garanciákat nyújtott, és csak azzal a feltétellel, hogy az érintettek számára érvényesíthető jogok és hatékony jogorvoslati lehetőségek rendelkezésre állnak. A Felügyeleti hatóság külön engedélye nélkül ilyen garanciák lehetnek különösen:

- a Bizottság által elfogadott általános adatvédelmi kikötések;
- a felügyeleti hatóság (NAIH) által elfogadott és a Bizottság által jóváhagyott általános adatvédelmi kikötések;

- a GDPR 40. cikke szerinti, jóváhagyott magatartási kódex a harmadik országbeli adatkezelő vagy adatfeldolgozó arra vonatkozó, kötelező erejű és kikényszeríthető kötelezettségvállalásával együtt, hogy alkalmazza a megfelelő garanciákat, ideértve az érintettek jogait illetően is;

- a GDPR 42. cikke szerinti, jóváhagyott tanúsítási mechanizmus a harmadik országbeli adatkezelő vagy adatfeldolgozó arra vonatkozó, kötelező erejű és kikényszeríthető kötelezettségvállalásával együtt, hogy alkalmazza a megfelelő garanciákat, ideértve az érintettek jogait illetően is;

- a felügyeleti hatóság engedélyével az adatkezelő és a harmadik országbeli adatkezelő, adatfeldolgozó vagy a személyes adatok címzettje között létrejött szerződéses rendelkezések.

25. Adatfeldolgozóként az adatkezelő támogatása az érintett jogainak biztosításában

25.1. A BKK, BKÜ, illetőleg a BÖK mint adatfeldolgozó támogatja az adatkezelőt abban, hogy képes legyen biztosítani az érintettnek az általános adatvédelmi rendeletben meghatározott jogaik érvényesítését.

25.1.1. A BKK, BKÜ, illetőleg a BÖK oly módon nyújtja szolgáltatását, hogy az adatkezelő az érintett igényére határidőben visszajelzést tudjon adni arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e.

25.1.2. A BKK, BKÜ, illetőleg a BÖK különösen oly módon nyújtja szolgáltatását, hogy az adatkezelő biztosítani tudja az érintett számára a személyes adat helyesbítéséhez, illetőleg törléséhez való jogot. Az adatkezelő kérésére a személyes adatot haladéktalanul véglegesen és helyreállíthatatlanul törölni/anonimizálni kell.

25.1.3. A BKK, BKÜ, illetőleg a BÖK különösen oly módon nyújtja szolgáltatását, hogy az adatkezelő biztosítani tudja az érintett számára az adatkezelés korlátozásához fűződő jogot.

25.1.4. A BKK, BKÜ, illetőleg a BÖK különösen oly módon nyújtja szolgáltatását, hogy az érintett az ügyfélhez mint adatkezelőhöz benyújtott kérelmet követően az adatkezelő rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja.

26. További-adatfeldolgozók

26.1. A BKK, BKÜ, illetőleg a BÖK adatfeldolgozóként eljárva kizárólag az adatkezelő (általános vagy eseti) előzetes írásos felhatalmazása/engedélye esetén vesz igénybe további adatfeldolgozót, és általános felhatalmazás esetén tájékoztatja az adatkezelőt minden olyan tervezett változásról, amely további adatfeldolgozók igénybevételét vagy azok cseréjét érinti.

26.2. További-adatfeldolgozó igénybevétele esetén a BKK, BKÜ, illetőleg a BÖK erre az adatkezelőre ugyanazon adatvédelmi kötelezettségeket telepíti, mint amelyeket az adatfeldolgozói szerződés szabályoz.

27. Incidenskezelés adatfeldolgozóként

27.1. Az adatvédelmi incidenst a BKK, BKÜ, illetőleg a BÖK adatfeldolgozóként eljárva a tudomására jutását követően indokolatlan késedelem nélkül bejelenti a megbízónak, mint adatkezelőnek.

27.2. A BKÜ és BÖK adatfeldolgozóként történő indicenskezelésére vonatkozó folyamat leírást a BKK, BKÜ, és a BÖK közös Incidenskezelési Folyamatleírása tartalmazza, mely jelen szabályzat mellékletét képez.

28. Az adatkezelői és adatfeldolgozói nyilvántartások

28.1. Adatkezeléseiről a BKK, BKÜ, és a BÖK köteles adatkezelési nyilvántartást vezetni a GDPR-ban foglaltak szerint.

28.2. Adatfeldolgozóként eljárva a BKK, BKÜ, és a BÖK köteles nyilvántartást vezetni az adatfeldolgozásairól a GDPR-ban foglaltak szerint.

III. ADATBIZTONSÁG

29. A számítástechnikai rendszerben tárolt adatok biztonsága

29.1. 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.

29.2. A fenti cél elérése érdekében az adatkezelések során - az adatkezelés jellegétől függően - az információs-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.

29.3. 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 személyes adatokat a BKK, BKÜ, illetőleg a BÖK szempontjából nézett 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 információ-feldolgozó 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 „bejelentkezve maradni", 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 kell,
- a személyes adat és az üzleti titok kategóriájába sorolt információt kinyomtatás vagy sokszorosítás után azonnal el kell távolítani a nyomtatóról és a fénymásolóból.

29.4. 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.

29.5. 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.

30. Hozzáférési jogosultság

30.1. A BKK, BKÜ és a BÖK 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.

30.2. A hozzáférési jogosultság szabályozásának alapját a személyes adatot és az üzleti titkot képező személyes 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.

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

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

30.5. 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).

30.6. 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.

30.7. 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.

30.8. 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 adatvédelmi tisztviselőjét.

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

31. Munkavállalói adatbiztonsági kötelezettségek

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

a) köteles az üzleti titok és a személyes adatok védelmére vonatkozó jogszabályi 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-nak, BKÜ-nek vagy a BÖK-nek, mint az adattal rendelkező jogosultnak, illetve adatkezelőnek haladéktalanul átadni.

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

31.3. 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.

31.4. A BKK, BKÜ és a BÖK valamennyi munkavállalója munkavégzése során köteles jelen Szabályzat rendelkezéseinek, előírásainak érvényt szerezni.

32. Titoktartási kötelezettség

32.1. A BKK, BKÜ és a BÖK-kel 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 leírásukban 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.

32.2 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.

32.3. 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.

33. A jogellenes adatkezelés következményei

33.1. 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.

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

34. Eljárási szabályok

34.1. Amennyiben a BKK, BKÜ, illetőleg a BÖK bármely szervezeti egysége, vagy szakterülete új típusú személyes adatkezelést határoz el, úgy erről az adatvédelmi jogszabályoknak való megfelelőséget vizsgáló konzultáció céljából köteles értesíteni az adatvédelmi tisztviselőt, a kezelendő személyes adatok típusának, a GDPR szerinti, az adatvédelmi nyilvántartásban meghatározandó információk megadásával. Az adatvédelmi tisztviselő – a vezérigazgatóval/ügyvezetővel való konzultációt követően, szükség szerint jogi állásfoglalás beszerzése után – gondoskodik az általános adatvédelmi rendeletben előírt intézkedések megtételéről (így az érdekmérlegelések jog terület általi kidolgozásáról, az adatvédelmi hatásvizsgálat lefolytatásáról, stb.) és bevezeti a változást adatkezelői vagy adatfeldolgozói nyilvántartásba vagy javaslatot tesz erre.

34.2. A BKK, BKÜ, illetőleg a BÖK részére érkező személyes adatokkal kapcsolatos igényeket, kérelmeket jogorvoslati kérelmeket haladéktalanul továbbítani kell az adatvédelmi tisztviselőnek.

34.3. Az adatvédelmi tisztviselő a kérést kivizsgálja, amelynek eredményéről – a BKK, BKÜ és a BÖK hatályos szabályzatainak megfelelően – értesíti a bejelentő személyt, a vezérigazgatót/ügyvezetőt és más érdekelteket.

34.4. Az adatvédelmi tisztviselő a személyes adattal kapcsolatos igények teljesítéséről, elutasításáról, annak időpontjáról és okáról nyilvántartást vezet.

34.5. A BKK, BKÜ és a BÖK adott szervezeti egységének vezetője a feladatkörébe tartozó egyes adatvédelmi folyamatok részletes szabályait külön munkautasításban szükséges szabályoznia.

35. Az adatvédelmi hatásvizsgálat általánosságban

35.1. A BKK, BKÜ, a BÖK, amennyiben az adatkezelés valamely (különösen új technológiákat alkalmazó) típusa, figyelemmel annak jellegére, hatókörére, körülményére és céljaira, valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, adatkezelést megelőzően hatásvizsgálatot végez arra vonatkozóan, hogy a tervezett adatkezelési műveletek a személyes adatok védelmét hogyan érintik. Olyan egymáshoz hasonló típusú adatkezelési műveletek, amelyek egymáshoz hasonló magas kockázatokat jelentenek, egyetlen hatásvizsgálat keretei között is értékelhetőek.

35.2. Hasonló típusú az adatkezelési művelet, ha:

- ugyanazon célból,
- ugyanazon típusú adatkezelés történik,
- hasonló technológia mellett.

35.3. A hatásvizsgálatot a BKK, a BKÜ, a BÖK azon szakterületének (nem az adatvédelmi tisztviselőnek) kell kezdeményeznie (nem egyetlen alkalommal, hanem változás esetén ismételten is) az adatvédelmi tisztviselőnél (a személyes adatkezelés tekintetében adatvédelmi hatásvizsgálat elvégzéséhez szükséges információk megadásával), amely az adott adatkezeléssel érintett feladatot végzi. A BKK érintett szakterülete az adatvédelmi hatásvizsgálatot az adatvédelmi tisztviselővel együtt végzi. Ha adatfeldolgozó igénybe vételére is sor kerül, akkor a hatásvizsgálatot az adatfeldolgozóval együtt kell elvégezni.

35.4. Az adatvédelmi hatásvizsgálatot különösen az alábbi esetekben kell elvégezni:

- természetes személyekre vonatkozó egyes személyes jellemzők olyan módszeres és kiterjedt értékelése, amely automatizált adatkezelésen - ideértve a profilalkotást is - alapul, és amelyre a természetes személy tekintetében joghatással bíró vagy a természetes személyt hasonlóképpen jelentős mértékben érintő döntések épülnek;
- a személyes adatok különleges kategóriái kezelése; illetve
- nyilvános helyek nagymértékű, módszeres megfigyelése.

35.5. Az olyan adatkezelési műveletek típusainak a jegyzékét - amelyekre vonatkozóan adatvédelmi hatásvizsgálatot kell végezni - a NAIH hatóság állítja össze és hozza nyilvánosságra. A felügyeleti hatóság összeállíthatja és nyilvánosságra hozhatja az olyan adatkezelési műveletek típusainak a jegyzékét is, amelyekre vonatkozóan nem kell adatvédelmi hatásvizsgálatot végezni.

35.6. A hatásvizsgálatnak legalább az alábbiakra kell kiterjednie:

- a tervezett adatkezelési műveletek módszeres leírására és az adatkezelés céljainak ismertetésére, beleértve adott esetben az adatkezelő által érvényesíteni kívánt jogos érdeket;
- az adatkezelés céljaira figyelemmel az adatkezelési műveletek szükségességi és arányossági vizsgálatára;
- az érintett jogait és szabadságait érintő kockázatok vizsgálatára;
- a kockázatok kezelését célzó intézkedések bemutatására, ideértve a személyes adatok védelmét és a GDPR-al való összhang igazolását szolgáló, az érintettek és más személyek jogait és jogos érdekeit figyelembe vevő garanciákat, biztonsági intézkedéseket és mechanizmusokat.

35.7. Az adatvédelmi hatásvizsgálat akkor van összhangban a GDPR rendelkezéseivel, ha

- módszeres leírás készült az adatfeldolgozásról;
- értékelésre került a szükségesség és az arányosság;
- az érintett jogait és szabadságait érintő kockázatok felmérésre kerültek, és ezen kockázatok orvoslására intézkedési terv született;
- az érdekeltek bevonásra kerültek.

35.8. Ha a BKK-ra, a BKÜ-re, a BÖK-re vonatkozó jogi kötelezettség teljesítéséhez szükséges adatkezelés jogalapját uniós vagy az adatkezelőre alkalmazandó tagállami jog írja elő, és e jog a szóban forgó konkrét adatkezelési műveletet vagy műveleteket is szabályozza, valamint e jogalap elfogadása során egy általános hatásvizsgálat részeként már végeztek adatvédelmi hatásvizsgálatot, akkor a hatásvizsgálatot nem kell ismételten elvégezni, kivéve, ha a tagállamok az adatkezelési tevékenységet megelőzően ilyen hatásvizsgálat elvégzését szükségesnek tartják.

35.9. A BKK-nak, a BKÜ-nek, a BÖK-nek szükség szerint, de legalább az adatkezelési műveletek által jelentett kockázat változása esetén ellenőrzést kell lefolytatnia annak értékelése céljából, hogy a személyes adatok kezelése az adatvédelmi hatásvizsgálatnak megfelelően történik-e.

35.10. Ha a hatásvizsgálat azt állapítja meg, hogy az adatkezelés a BKK, a BKÜ, a BÖK által a kockázat mérséklése céljából tett intézkedések hiányában valószínűsíthetően magas kockázattal jár, a személyes adatok kezelését megelőzően szükséges konzultálni a NAIH-al.

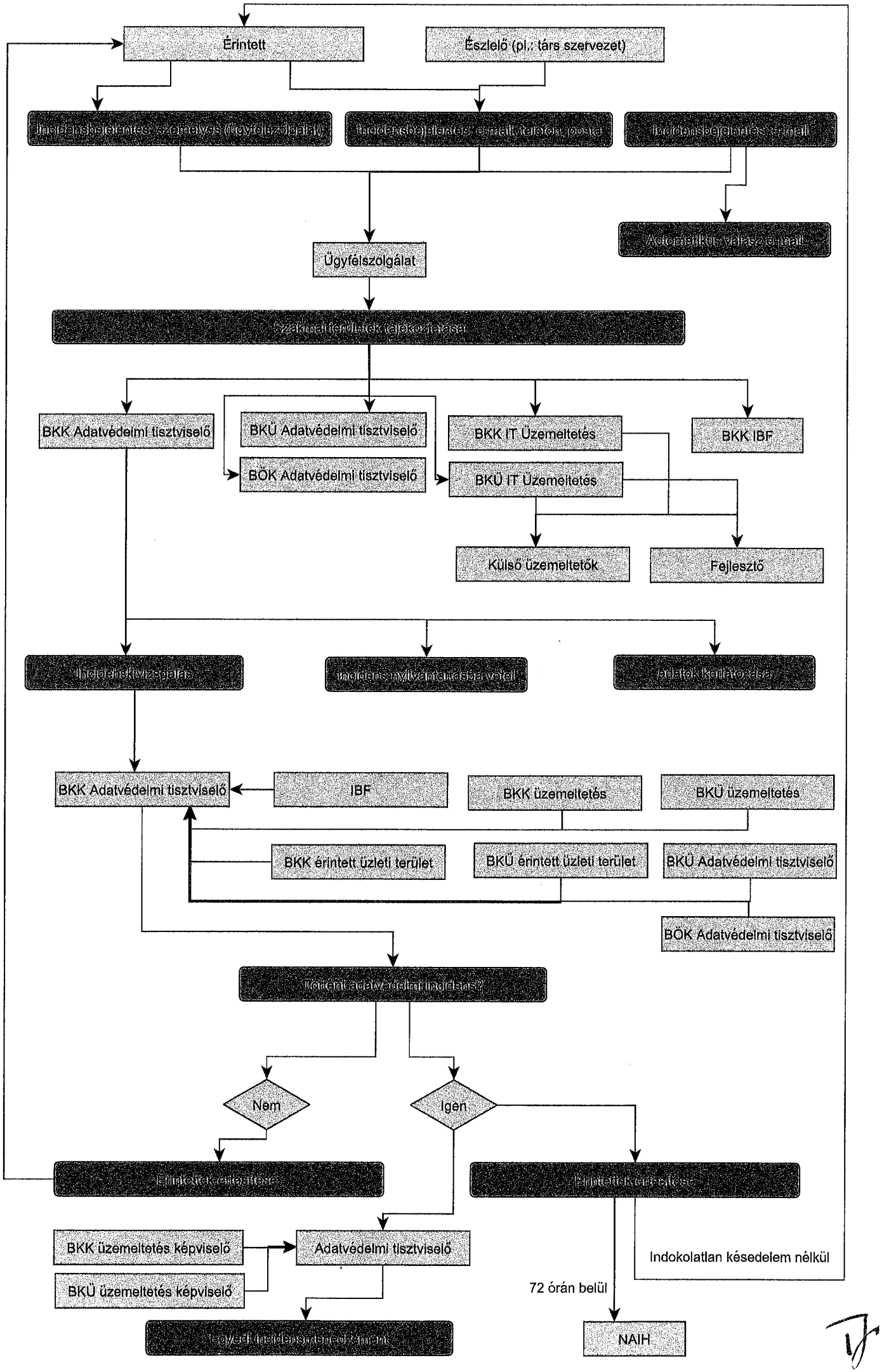
35.11. Az adatvédelmi hatásvizsgálat részletesebb szabályairól a BKK, a BKÜ, a BÖK külön szabályzatot alkothat.

36. Adatvédelmi audit

A jelen szabályzatban meghatározott követelmények teljesülése rendszeres ellenőrzések tárgya, ennek megfelelően az adatvédelmi tisztviselő az adatkezelésért felelős szervezeti egységgel együttműködve biztosítja, hogy a követelmények teljesülése, illetve a lefolytatott ellenőrzések megfelelően dokumentáltak és nyomon követhetők legyenek a további belső és az esetleges külső ellenőrzések során is.

Az ún. adatvédelmi audit (ellenőrzés) részletes szabályait, az ezzel összefüggő tevékenységeket, felelősségeket a BKK, a BKÜ, a BÖK erre vonatkozó külön szabályzatban határozhatja meg.

Melléklet: Incidenskezelési Folyamatábra (ábra)


Érintett
Észlelő (pl.: társ szervezet)
Incidensbejelentés személyes (ügyfélszolgálat)
Incidensbejelentés e-mail, telefon, poszta
Incidensbejelentés e-mail
Automatikus válasz e-mail
Ügyfélszolgálat
Szakmai területek tájékoztatása
BKK Adatvédelmi tisztviselő
BKÜ Adatvédelmi tisztviselő
BÖK Adatvédelmi tisztviselő
BKK IT Üzemeltetés
BKÜ IT Üzemeltetés
BKK IBF
Külső üzemeltetők
Fejlesztő
Incidens kivizsgálás
Incidens nyilvántartásba vétel
Adatok korlátozása
BKK Adatvédelmi tisztviselő
IBF
BKK üzemeltetés
BKÜ üzemeltetés
BKK érintett üzleti terület
BKÜ érintett üzleti terület
BKÜ Adatvédelmi tisztviselő
BÖK Adatvédelmi tisztviselő
Történt adatvédelmi incidens?
Nem
Igen
Érintettek értesítése
Érintettek értesítése
BKK üzemeltetés képviselő
BKÜ üzemeltetés képviselő
Adatvédelmi tisztviselő
Indokolatlan késedelem nélkül
72 órán belül
Hatósági incidensbejelentés
NAIH