BUDAPESTI KÖZLEKEDÉSI KÖZPONT

44/2024/VIG/CO/1 sz. Vezérigazgatói utasítás

a BKK Zrt. személyes adatkezelési és adatvédelmi 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
web: www.bkk.hu
e-mail: bkk@bkk.hu
iktató szám: 1167/74-1/2024/1167

Tartalomjegyzék

BEVEZETÉS

A BKK Budapesti Közlekedési Központ Zártkörűen Működő Részvénytársaság (a továbbiakban: BKK, Társaság vagy Adatkezelő) az információs önrendelkezési jogról és az információszabadságról szóló 2011. CXII. törvény (a továbbiakban: Info tv.), valamint az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet; a továbbiakban: GDPR) rendelkezéseivel összhangban, a személyes adatok védelmének biztosítása érdekében az alábbiak szerint alkotja meg a személyes adatkezelésre és adatvédelemre vonatkozó szabályzatát (a továbbiakban: Szabályzat).

A jelen Szabályzat tartalmazza a BKK személyes adatkezeléseire vonatkozó előírásokat, eleget téve az alkalmazandó jogszabályok követelményeinek, valamint meghatározza az érintettek jogainak védelme érdekében a Társaságtól megkövetelt technikai és szervezési intézkedéseket, elvárásokat.

Jelen Szabályzat a gyakorlati alkalmazásához tartozó módszertani ismereteket és mintadokumentumokat is tartalmazza.

1. ÁLTALÁNOS RENDELKEZÉSEK

1.1. A Szabályzat célja és hatálya

1) A Szabályzat célja, hogy a BKK tevékenysége során biztosítsa a kezelt személyes adatok védelmét, meghatározza a személyes adatok kezelése során irányadó adatvédelmi előírásokat, biztosítsa a személyes adatokat tartalmazó nyilvántartások jogszabályoknak megfelelő működési rendjét, az adatvédelem alkotmányos elveinek, az adatbiztonság követelményeinek érvényesülését, valamint megakadályozza a személyes adatokhoz való jogosulatlan hozzáférést, azok jogosulatlan megváltoztatását vagy nyilvánosságra hozatalát.

2) A Szabályzat személyi hatálya kiterjed a BKK valamennyi szervezeti egységére, a Társaság összes munkavállalójára, továbbá a BKK szerződött adatfeldolgozóira, annak munkavállalóira, továbbá azokra a személyekre, akik a BKK által kezelt személyes adatokkal valamilyen módon kapcsolatba kerülnek (természetes és jogi személyek, jogi személyiséggel nem rendelkező szervezetek stb.), beleértve azokat is, akik a BKK-val szerződéses jogviszonyban állnak.

3) A Szabályzat tárgyi hatálya kiterjed a BKK által bármely célból kezelt személyes adatra és a személyes adatoknak a Társaságnál megtalálható valamennyi nyilvántartására, függetlenül azok megjelenési formájától.

1.2. Értelmező rendelkezések

4) Jelen Szabályzat alkalmazásában:

a) Adatállomány: az egy adatkezelési nyilvántartásban kezelt személyes adatok összessége.

b) Adatbiztonság: a személyes adatok védelme – különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás – érdekében megtett technikai és szervezési intézkedések, kialakított eljárási szabályok összessége.

c) Adatfeldolgozás: az Adatkezelő megbízásából, vagy rendelkezése alapján eljáró adatfeldolgozó által végzett adatkezelési műveletek összessége.

d) Adatfeldolgozó: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az Adatkezelő nevében személyes adatokat kezel.

e) Adatkezelés: 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.

f) Adatkezelés korlátozása: a tárolt személyes adatok megjelölése jövőbeli kezelésük korlátozása céljából.

g) 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.

h) Adatkezelési Nyilvántartás: az Adatkezelő által végzett összes adatkezelési tevékenység nyilvántartása a GDPR 30. cikkében meghatározott tartalommal.

i) Adatkezelési Tájékoztató: a személyes adatok kezelésére vonatkozóan a GDPR 12-14. cikkeiben meghatározott, az Érintettek részére az adatkezelés megkezdését megelőzően, a GDPR-ban meghatározott kötelező tartalommal rendelkezésre bocsátandó információk összessége.

j) Adatkezelési tevékenységek: a Társaság által végzett azon adatkezelési műveletek összessége, amelyek meghatározott adatkezelési cél érdekében, a GDPR-ban meghatározott jogalappal történnek.

k) Adatkezelési tevékenységért felelős szervezeti egység: az egyes adatkezelési célokhoz kapcsolódó adatkezelési tevékenységért felelős szervezeti egység.

l) Adatmegsemmisítés: az adatot tartalmazó adathordozó teljes fizikai megsemmisítése.

m) Adattovábbítás: az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele.

n) Adattörlés: az adat felismerhetetlenné tétele oly módon, hogy a helyreállítása többé nem lehetséges.

o) Adatvédelmi koordinátor: az egyes szervezeti egységekben annak vezetője által kijelölt munkavállaló, aki az adott szervezeti egység vonatkozásában adatvédelmi kérdésekben a Compliance osztállyal szoros kapcsolatot tart, valamint jelen szabályzat 2.3.3 pontjában részletezettek szerint aktívan közreműködik az adatkezelési tevékenységek koordinálásában és az adatkezelési tevékenységekre vonatkozó feladatok ellátásában.

p) 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.

q) Adatvédelmi tisztviselő, DPO: Data Protection Officer, a GDPR 37-39. cikke szerinti személy, aki a Társaság adatvédelmi jogszabályoknak megfelelő működéséről gondoskodik, az adatkezelési tevékenységeket ellenőrzi és adatvédelmi kérdésekben állást foglal.

r) 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. Az álnevesített adatok kezelésére a GDPR rendelkezéseit alkalmazni kell.

s) Anonimizálás: az a folyamat, melynek célja, hogy a személyes adatokat olyan módon alakítsa át, amelynek következtében az érintett nem vagy többé nem azonosítható. A GDPR nem vonatkozik az anonim információk kezelésére, a statisztikai vagy kutatási célú adatkezelést is ideértve.

t) Címzett: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, akivel vagy amellyel a személyes adatot közlik, függetlenül attól, hogy harmadik fél-e. Azon közhatalmi szervek, amelyek egy egyedi vizsgálat keretében az uniós vagy a tagállami joggal összhangban férhetnek hozzá személyes adatokhoz, nem minősülnek címzettnek.

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

v) Érintett: az a természetes személy, akire vonatkozóan az Adatkezelő személyes adatot kezel.

w) Érintett hozzájárulása: az Érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló, egyértelmű kinyilvánítása, amellyel nyilatkozat vagy a megerősítést

félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez.

x) Felügyeleti Hatóság: egy tagállam által a GDPR 51. cikkének megfelelően létrehozott független közhatalmi szerv; Magyarországon a Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: NAIH).

y) GDPR: AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet).

z) 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**.**

aa) Harmadik ország: minden olyan állam, amely nem EGT-állam.

bb) Különleges adat: a személyes adatok különleges kategóriáiba tartozó minden adat, azaz a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a genetikai adatok, a természetes személyek egyedi azonosítását célzó biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok.

cc) NAIH: Nemzeti Adatvédelmi és Információszabadság Hatóság.

dd) Nyilvánosságra hozatal: a személyes adat bárki számára történő hozzáférhetővé tétele.

ee) Nyilvántartási rendszer: a személyes adatok bármely módon – centralizált, decentralizált, funkcionális vagy földrajzi szempontok szerint – tagolt állománya, amely meghatározott ismérvek alapján hozzáférhető.

ff) 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.

gg) 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.

1.3. Adatkezelési alapelvek

5) A személyes adatok kezelése során a Társaság a GDPR 5. cikkében és az Info tv. 4. §-ában meghatározott alábbi alapelvek szerint köteles eljárni:

a) a személyes adatokat jogszerűen és tisztességesen, valamint az Érintett számára átlátható módon kell kezelnie;

b) személyes adatokat csak meghatározott, egyértelmű és jogszerű célból, jog gyakorlása vagy kötelezettség teljesítése érdekében kezelhet;

c) csak az adatkezelés célja szempontjából megfelelő és releváns személyes adatokat kezelhet, a cél eléréséhez feltétlenül szükséges mértékben és ideig, biztosítva az adattakarékosság érvényesülését;

d) biztosítja a személyes adatok pontosságát, teljességét és szükség esetén naprakészségét, valamint minden ésszerű intézkedést megtesz annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul töröljék vagy helyesbítsék;

e) a személyes adatokat olyan formában tárolja, amely az Érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé, biztosítva ezzel a korlátozott tárolhatóságot;

f) az integritás és bizalmas jelleg alapelvének megfelelő technikai és szervezési intézkedéseket alkalmaz az adatbiztonság érdekében, ennek körében a személyes adatok kezelése során védi azokat a jogosulatlan vagy jogellenes kezeléssel, a véletlen elvesztéssel, a megsemmisítéssel vagy károsodással szemben,

g) a személyes adatok kezelését az elszámoltathatóság alapelvének megfelelően olyan módon végzi és dokumentálja, hogy képes legyen a fenti alapelveknek való megfelelés igazolására.

1.4. Az adatkezelés jogszerűsége

6) A GDPR 6-9. cikkei adják meg az adatkezelés jogszerűségének általános szabályait, ezek betartása a Társaságra nézve kötelező.

7) A megfelelő jogalap alkalmazása olyan feltétel, amely elengedhetetlenül szükséges a jogszerű adatkezeléshez. A személyes adatok jogszerű kezeléséhez szükséges részletes szabályokat jelen szabályzat 2.1 pontja tartalmazza.

1.5. Érintettek jogainak védelme

8) Az Érintettek jogérvényesítésének, jogaik védelmének elősegítése érdekében az Adatkezelő köteles átlátható, közérthető tájékoztatást adni az adatkezeléseiről, valamint köteles biztosítani az Érintettek részére az adatokhoz való hozzáférést, a helyesbítéshez, törléshez, adatkezelés korlátozásához, az adathordozhatósághoz, valamint a tiltakozáshoz való jogot a GDPR 12-22. cikke szerinti szabályok szerint.

9) Az Érintettek jogaira és az érintetti kérelmekre vonatkozó részletes szabályokat jelen szabályzat 2.2. pontja tartalmazza.

1.6. Az adatvédelmi intézményrendszer szereplői

10) A BKK jogszabályoknak megfelelő adatvédelmi működését, a személyes adatkezelési és adatvédelmi feladatok jogszabályoknak megfelelő végrehajtását a BKK-nál háromszintű rendszer biztosítja:

1. szint Az Adatvédelmi tisztviselő, mely feladatkört vezérigazgatói döntés alapján a BKK saját munkavállalója, vagy külső megbízott látja el.

2. szint A személyes adatvédelmi és adatkezelési tevékenységek Társaságon belüli koordinálását, valamint, ha az Adatvédelmi tisztviselő feladatait külső megbízott látja el, az Adatvédelmi tisztviselővel történő mindennapi operatív kapcsolattartást a Compliance Osztály látja el.

3. szint Minden szervezeti egységben Adatvédelmi koordinátor kerül kijelölésre a BKK adott szervezeti egységének adatkezelési céljaival kapcsolatos feladatok ellátására.

11) A GDPR-ban az Adatvédelmi tisztviselő számára előírt feladatokat a Compliance Osztály, valamint az Adatvédelmi koordinátorok együttműködésével és közreműködésével az Adatvédelmi tisztviselő végzi, melynek keretében ellenőrzi a BKK GDPR-nak, egyéb uniós vagy hazai szabályozásnak, rendelkezésnek, a jelen szabályzatnak és az adatvédelemmel összefüggő egyéb szabályozóknak való megfelelését.

12) Az adatkezelési feladatokat ellátó szereplők tevékenységének részletes leírását jelen szabályzat 2.3. pontja tartalmazza.

1.7. Nyilvántartási és dokumentációs kötelezettség

13) Az átláthatóság és elszámoltathatóság alapelvének megfelelően az Adatkezelő adatkezeléssel kapcsolatos tevékenységeit teljeskörűen dokumentálja, amely magában foglalja az adatkezeléssel kapcsolatos – GDPR-ban, valamint jelen szabályzatban előírt kötelező – nyilvántartások vezetését. A BKK köteles lehetővé tenni, hogy a Felügyeleti Hatóság ellenőrizni tudja a Társaság adatkezelési tevékenységét érintő jogszabályi megfelelést.

14) A BKK adatkezeléssel és adatvédelemmel kapcsolatos nyilvántartásait az Adatvédelmi koordinátor tájékoztatása és adatszolgáltatása alapján a Compliance Osztály vezeti jelen szabályzat 2.4. pontjában meghatározott módszertan alapján.

1.8. Közös adatkezelési és adatfeldolgozási jogviszony

15) A BKK, mint Adatkezelő, Adatfeldolgozókat alkalmazhat, vagy másokkal közös adatkezeléseket folytathat. A Társaság kizárólag olyan Adatfeldolgozókat vehet igénybe, vagy olyan Adatkezelőkkel folytathat közös adatkezeléseket, akik a szerződés teljesítése során mindvégig biztosítják a GDPR előírásainak történő megfelelést és annak rendelkezéseit önmagukra nézve kötelező érvényűnek tekintik.

16) A Társasággal jogviszonyban álló, adatkezelést vagy adatfeldolgozást végző személyek felelősséggel tartoznak minden olyan kárért, amely adatkezelési, adatvédelmi kötelezettségük megszegéséből származik.

17) A BKK az Adatfeldolgozókkal az adatfeldolgozás részletes feltételeiről írásban köteles adatfeldolgozói megállapodást kötni. Az adatfeldolgozói megállapodást jelen szabályzat 1. számú melléklete szerinti minta alkalmazásával készítik el a felek.

18) A Társaság az adatfeldolgozási jogviszonnyal is járó (köz)beszerzései tekintetében a szerződéskötéssel egyidejűleg köteles az adatfeldolgozási megállapodást is megkötni, amely a (köz)beszerzési eljárás során megkötendő szerződés mellékletét képezi.

19) A Compliance Osztály az adatfeldolgozói megállapodásokról nyilvántartást vezet.

20) Amennyiben a fentiektől eltérően az eset összes körülményét figyelembe véve a jogviszony nem adatfeldolgozói jogviszonynak, hanem közös adatkezelésnek minősül, akkor az Adatkezelő és a további Adatkezelők a közöttük létrejött megállapodásban (közös adatkezelői megállapodás) kötelesek meghatározni a GDPR-ban foglalt kötelezettségek teljesítéséért fennálló felelősségük megoszlását, különösen az érintettek jogainak

gyakorlásával és tájékoztatásával kapcsolatban. A megállapodásban minden esetben meg kell jelölni, hogy melyik Adatkezelő tartja a kapcsolatot az Érintettel.

21) Az adatfeldolgozói megállapodást, valamint a közös adatkezelői megállapodást a DPO bevonásával kell előkészíteni, aki a megállapodás tervezetét minden esetben véleményezi, továbbá a kész dokumentumot aláírás előtt szignózza.

22) Az adatkezelési viszonyt szabályozó szerződésekben külön rögzíteni kell a felek szerepét, feladat és hatásköreit adatvédelmi incidens bekövetkezése esetén. Ezekben elő kell írni, hogy az adatfeldolgozó az adatvédelmi incidenst, az arról való tudomásszerzését követően indokolatlan késedelem nélkül bejelenti az adatkezelőnek.

1.9. Az adatvédelmi incidens

23) Az adatok biztonságát megvalósító technikai és szervezési intézkedések ellenére bekövetkező adatvédelmi incidensek kezelése és elhárítása, az adatbiztonsági sérülések lehető legrövidebb időn belüli, és az esetleges következményként előálló kár kockázatainak minimalizálása a Társaság, mint Adatkezelő kötelezettsége.

24) Az adatvédelmi incidensekkel kapcsolatos általános szabályokat, valamint a bekövetkezett adatvédelmi incidensek kezelésére vonatkozó részletes szabályokat a mindenkor hatályos Adatvédelmi incidenskezelés eljárásrendről szóló vezérigazgatói utasítás tartalmazza.

1.10. Jogorvoslati lehetőségek

25) A BKK-nak, mint Adatkezelőnek az Érintettek számára biztosítania kell jogellenes adatkezelés esetén a megfelelő jogorvoslati lehetőségeket.

26) A Magyarországon illetékes Felügyeleti Hatóság megnevezését és elérhetőségét az egyes Adatkezelési Tájékoztatóknak tartalmazniuk kell.

1.11. Adatvédelmi tudatosság-növelése és fenntartása

27) Az adatvédelmi tudatosság növelése érdekében a Társaság kijelölt munkavállalói és az Adatvédelmi koordinátorok számára évente adatvédelmi tudatosság fenntartását célzó képzéseket kell tartani. Az oktatások megszervezéséről és megtartásáról – a Compliance Osztály közreműködése mellett – a Képzés szakterület gondoskodik az Adatvédelmi tisztviselő által kiadott oktatási tananyag alapján (e-learning szervezésével, vagy szóbeli oktatás esetén az Adatvédelmi tisztviselő bevonásával).

2. RÉSZLETES SZABÁLYOK

2.1. A személyes adatok jogszerű kezelése

2.1.1. Jogalapok

28) Személyes adatot a BKK, mint Adatkezelő kizárólag az alábbi esetekben kezelhet:

a) ha az Érintett hozzájárulását adta az adatainak kezeléséhez, vagy

b) ha az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az Érintett az egyik fél, vagy a szerződés megkötését megelőzően az Érintett kérésére történő lépések megtételéhez szükséges, vagy

c) ha az adatkezelés az Adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges, vagy

d) ha az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges, vagy

e) ha az adatkezelés az Érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges, vagy

f) ha az adatkezelés az Adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az Érintett olyan érdekei vagy alapvetői jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé, különösen, ha az Érintett gyermek.

2.1.2. A megfelelő jogalap meghatározása

29) A BKK a (GDPR 6. cikk (1) bekezdés a)-f) pontjaiban foglaltak szerint) jelen szabályzat 2.1.1 bekezdésében meghatározott jogalapok valamelyikére alapozhatja adatkezelésének jogszerűségét.

30) A jogalapok között nincs hierarchia, az adott adatkezelési tevékenységhez legmegfelelőbb jogalapot kell minden esetben megtalálni.

31) A megfelelő jogalap meghatározása csak az egyik eleme a jogszerű adatkezelésnek. Emellett az adatkezelés alapelveinek (átlátható, jogszerű, tisztességes adatkezelés, célhoz kötöttség, adattakarékosság, korlátozott tárolhatóság, pontosság, integritás és bizalmas jelleg) is érvényesülniük kell minden esetben.

32) Különleges személyes adatok tekintetében a főszabály az adatkezelés tilalma, amely akkor oldható fel, ha a GDPR 6. cikkében meghatározott valamely jogalap érvényesülésén túl a 9. cikk (2) bekezdésében meghatározott valamely további feltétel is fennáll.

2.1.3. Az egyes jogalapok részletes ismertetése

2.1.3.1. Az Érintett hozzájárulása

33) Az Érintett érvényes hozzájárulásával szemben támasztott követelmények:

a) az Adatkezelőnek képesnek kell lennie annak igazolására, hogy az Érintett személyes adatainak kezeléséhez hozzájárult;

b) ha a hozzájárulás megadása olyan írásbeli nyilatkozattal történik, amely más ügyekre is vonatkozik, a hozzájárulás iránti kérelmet ezektől az ügyektől egyértelműen megkülönböztethető módon kell előadni, érthető és könnyen hozzáférhető formában, világos és egyszerű nyelvezettel;

c) az Érintett jogosult arra, hogy hozzájárulását bármikor visszavonja. A hozzájárulás visszavonása nem érinti a hozzájáruláson alapuló, a visszavonás előtti adatkezelés jogszerűségét. A hozzájárulás megadása előtt az Érintettet erről tájékoztatni kell. A hozzájárulás visszavonását ugyanolyan egyszerű módon kell lehetővé tenni, mint annak megadását;

d) annak megállapítása során, hogy a hozzájárulás önkéntes-e, figyelembe kell venni, hogy a szerződés teljesítésének (beleértve a szolgáltatások nyújtását is) feltételéül szabták-e az olyan személyes adatok kezeléséhez való hozzájárulást, amelyek nem szükségesek a szerződés teljesítéséhez.

34) Amennyiben az adatkezelés valamely lényeges eleme megváltozik, akkor a hozzájárulás megújítása válhat szükségessé, illetve szükséges a hozzájárulások megújítása bizonyos időközönként is. Az adatkezelés lényeges elemének megváltozásáról az Adatkezelésért felelős szervezeti egység minden esetben köteles tájékoztatni a Compliance Osztályt. A hozzájárulás megújításának szükségességéről minden esetben a DPO dönt.

2.1.3.2. A szerződés teljesítése

35) A szerződés teljesítése, olyan adatkezelések esetében alkalmazható jogalap, ahol a kezelt személyes adatok ténylegesen szükségesek a szerződés teljesítéséhez.

36) A jogalap nem alkalmazható olyan helyzetekre, ahol az adatkezelés valójában nem a szerződés teljesítéséhez szükséges, hanem azt az Adatkezelő egyoldalúan az Érintettre erőlteti.
37) A szerződés teljesítéséhez kapcsolódó jogalap kizárólag akkor alkalmazható, ha az Érintett, akinek a személyes adatait a szerződés alapján, vagy annak előkészítése érdekében kezelni kívánja az Adatkezelő, a szerződés alanya. Közvetlen szerződéses kapcsolat hiányában ez a jogalap nem alkalmazható.
38) A szerződést megelőzően erre a jogalapra alapított adatkezelések nem lehetnek olyanok, amelyeket az Adatkezelő kezdeményez (a GDPR szerint *"[...] az a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges"*).

2.1.3.3. Jogi kötelezettség teljesítése

39) Jogi kötelezettségre alapított adatkezelés esetén az Adatkezelőnek meg kell tudnia határozni azt a rá vonatkozó uniós vagy tagállami jogi kötelezettséget, amelyre az adatkezelést alapítják. Az ezzel kapcsolatos részletes követelményeket a GDPR 6. cikk (3) bekezdése határozza meg.
40) A jogi kötelezettség teljesítéshez szükséges adatkezelések esetében is vizsgálni kell az adatkezeléssel kapcsolatos további feltételek megvalósulását, különös tekintettel a szükségesség-arányosság követelményeire.

2.1.3.4. Létfontosságú érdek

41) Különleges helyzetekre alkalmazható jogalap az Érintett vagy másik természetes személy létfontosságú érdekeinek védelme érdekében történő adatkezelés.
42) A létfontosságú érdek jogalap a természetes személy életének védelme vagy más kiemelten fontos érdek védelme, veszély megelőzése érdekében alkalmazható.
43) Olyan atipikus helyzetekben alkalmazható, amikor más jogalap nem megfelelő. A létfontosságú érdek, mint jogalap tipikusan kisebb mértékű adatkezelések esetében alkalmazható elsődlegesen, nagyobb volumenű adatkezelések alapja csak kivételesen lehet.

2.1.3.5. Közérdekű feladatok vagy közhatalmi jogosítványok gyakorlása keretében végzett feladatok végrehajtásához szükséges adatkezelés

44) Közérdekű feladatok vagy közhatalmi jogosítványok gyakorlása keretében végzett feladatok végrehajtásához szükséges jogalapra kizárólag akkor lehet hivatkozni, amennyiben

az adatkezelés a közérdekű feladat vagy az Adatkezelőre ruházott közhatalmi jogosítvány gyakorlása keretében végzett feladat végrehajtásához szükséges, valamint az adatkezelés jogalapját az uniós jog, vagy azon tagállami jog állapítja meg, amelynek hatálya alá az Adatkezelő tartozik.

45) Az adatkezelés célját e jogalapra hivatkozással kell meghatározni, illetve az adatkezelés tekintetében annak szükségesnek kell lennie valamely közérdekű vagy az Adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához.

2.1.3.6. Jogos érdek

46) Az adatkezelés jogos érdekre hivatkozással akkor jogszerű, ha az adatkezelés az Adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges.

47) A jogos érdeken alapuló adatkezelés egyik fő funkciója, hogy az adatkezelések kapcsán a rugalmasságot biztosítsa az Adatkezelő számára, mert ez a jogalap alkalmazható olyan esetekben, amikor az adatkezelés nem illik más adatkezelési jogalapok keretei közé.

48) Jogos érdeken alapuló adatkezelés megkezdését megelőzően kötelező az Érintettek és az Adatkezelők érdekeinek a megfelelő számbavétele, és annak vizsgálata, hogy az adatkezelés nem jelent-e túlzott beavatkozást az Érintett magánszférájába, illetve nem okoz-e aránytalan sérelmet a számára. Ezt az ún. érdekmérlegelési teszt keretében szükséges elvégezni és dokumentálni, mely az elszámoltathatóság elvére tekintettel kötelező.

2.1.4. A jogalapokkal kapcsolatos jogszabályi dokumentációs kötelezettség

49) Az egyes adatkezelési tevékenységek jogalapjait az Adatkezelési Nyilvántartás és az annak alapján készített Adatkezelési Tájékoztatók tartalmazzák.

2.1.4.1. Hozzájárulás

50) Ha az Adatkezelési Nyilvántartás a hozzájárulást jelöli meg az adatkezelés jogalapjaként, akkor az elszámoltathatóság alapelvére tekintettel az Adatkezelőnek képesnek kell lennie annak igazolására, hogy az Érintett a személyes adatainak kezeléséhez előzetes, önkéntes, konkrét és megfelelő tájékoztatáson alapuló egyértelmű kinyilvánításával hozzájárult, azaz nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelezte, hogy beleegyezését adta az őt érintő személyes adatok kezeléséhez.

51) Hozzájárulás jogalap esetén személyes adat kizárólag az Érintett dokumentált – ideértve az elektronikus utat is – nyilatkozatát követően kezelhető. Az írásbeli hozzájárulás kötelező tartalmi elemeit jelen szabályzat 2. számú melléklete tartalmazza.
52) Az elektronikus úton (pl. checkbox bekattintása) beszerezni kívánt hozzájárulás tartalmáról az Adatkezelésért felelős szervezeti egység minden esetben előzetesen egyeztet a Compliance osztállyal.

2.1.4.2. Érdekmérlegelési teszt

53) Amennyiben az Adatkezelési Nyilvántartás jogos érdeket jelöl meg az adatkezelés jogalapjaként, akkor érdekmérlegelési tesztet kell készíteni.
54) Az elszámoltathatóság alapelvére tekintettel jogos érdek jogalap esetén személyes adat csak érdekmérlegelés elvégzését és írásbeli dokumentálását követően kezelhető.
55) Érdekmérlegelés keretében meg kell határozni, hogy mi alkotja az Adatkezelő vagy a harmadik fél jogszerű érdekét, és meg kell vizsgálni, hogy mi alkotja az Érintett olyan érdekeit vagy alapvető jogait és szabadságait, amelyek a személyes adatok védelmét teszik szükségessé.
56) Az érdekmérlegelési teszt mintáját jelen szabályzat 3. számú melléklete tartalmazza.
57) Az érdekmérlegelési teszteket az adatkezelés megkezdését megelőzően az Adatkezelési tevékenységért felelős szervezeti egység készíti elő szakmai szempontok alapján. Az adatvédelmi szakmai kérdések tekintetében a Compliance az Adatkezelési tevékenységért felelős szervezeti egységgel együttműködik. Az adatkezelés kizárólag az érdekmérlegelési teszt Adatvédelmi tisztviselő általi jóváhagyását követően kezdhető meg.

2.1.4.3. Adatvédelmi hatásvizsgálat

58) Az Adatkezelőnek az adatkezelést megelőzően hatásvizsgálatot kell végeznie a GDPR 35. cikkének megfelelően, a Felügyeleti Hatóság erre vonatkozó jegyzékének figyelembevételével, ha az adatkezelés valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve. Különösen az új adatkezelési technológiák használatba vételét megelőzően szükséges megvizsgálni jelen szabályzat 4. számú mellékletében megadott, NAIH által javasolt módszertan és minta szerint, hogy a tervezett adatkezelési műveletek hogyan érintik a személyes adatok védelmét.
59) Az adatvédelmi hatásvizsgálatot az Adatkezelésért felelős szervezeti egység szakmai szempontok alapján – az Adatvédelmi koordinátor bevonásával, valamint a Compliance

Osztály adatvédelmi szakmai támogatása és együttműködése mellett – végzi el. A hatásvizsgálat során az Adatvédelmi tisztviselő szakmai tanácsát minden esetben ki kell kérni.

2.2. Érintettek jogérvényesítése, jogainak védelme

2.2.1. Átlátható tájékoztatás és kommunikáció (GDPR 13-14. cikk)

60) Az Adatkezelő az Érintettek részére a személyes adatok kezelésére vonatkozó minden információt tömör, átlátható, érthető és könnyen hozzáférhető módon, világosan és közérthetően megfogalmazva nyújtja. A tájékoztatást írásban vagy más módon – ideértve az elektronikus utat is – kell megadni.

61) A tájékoztatás jogának gyakorlása a GDPR 13. cikk (4) bekezdés szerint – amennyiben az adatok forrása az Érintett – megtagadható, ha az Érintett már rendelkezik az előírt információkkal.

62) A tájékoztatás jogának gyakorlása a GDPR 14. cikk (5) bekezdése értelmében – amennyiben a személyes adatokat nem az Érintettől szerezték meg – az alábbi esetekben tagadható meg:

a) az Érintett már rendelkezik az előírt információkkal;

b) a rendelkezésre bocsátás lehetetlen, aránytalanul nagy erőfeszítést igényel vagy a rendelkezésre bocsátás ténye lehetetlenné tenné vagy veszélyeztetné az adatkezelés céljának elérését (amelyre vonatkozóan az Adatkezelési Nyilvántartásnak külön jelölést kell tartalmaznia) és amelynek érdekében az Adatkezelő megfelelő intézkedéseket hozott az Érintett jogos érdekeinek védelme érdekében;

c) kifejezett olyan jogszabályi előírás esetén, amely egyidejűleg az Érintett jogos érdekeinek védelméről is rendelkezik;

d) ha a jogszabályban előírt szakmai titoktartási kötelezettség vagy jogszabályon alapuló titoktartási kötelezettség miatt az adatkezelésnek bizalmasnak kell maradnia (amelyre vonatkozóan az Adatkezelési Nyilvántartásnak külön jelölést kell tartalmaznia).

2.2.2. Az érintettek jogai

2.2.2.1. Tájékoztatáshoz való jog

63) A jogszabálynak megfelelő, a GDPR 13. és 14. cikkében előírt kötelező elemeket tartalmazó Adatkezelési Tájékoztató mintáját a jelen szabályzat 5. számú melléklete tartalmazza.

64) Az Adatkezelési Tájékoztatók előkészítése, mely magában foglalja az adatkezelési célok, valamint a kezelt személyes adatok precíz, pontos meghatározását, az Adatkezelési tevékenységért felelős szervezeti egység feladata és felelőssége. Az előkészített Adatkezelési Tájékoztatót a Compliance Osztály a GDPR-nak történő megfelelés érdekében megvizsgálja és az Adatkezelési tevékenységért felelős szervezeti egységtől kapott információk alapján a szükséges adatvédelmi szakmai rendelkezésekkel kiegészíti. Az Adatkezelési Tájékoztatót az Adatvédelmi tisztviselő hagyja jóvá. A jóváhagyást követően – amennyiben szükséges – a Compliance Osztály intézkedik az Adatkezelési Tájékoztató BKK honlapjára, illetve a BKK intranetre történő publikálásáról.

65) Az Adatkezelési Tájékoztató Érintettekkel történő megismertetése az Adatkezelési tevékenységért felelős szervezeti egység feladata.

66) Az Adatkezelési Tájékoztatót az Érintettel a személyes adatok kezelésének konkrét körülményeit figyelembe véve az alábbiak szerint közli az Adatkezelési tevékenységért felelős szervezeti egység:

a) ha az Érintettől szerezték meg a személyes adatokat, akkor a személyes adatok megszerzésének időpontjában;

b) ha nem az Érintettől szerezték meg a személyes adatokat, akkor a megszerzésétől számított ésszerű határidőn, de legkésőbb egy hónapon belül és díjmentesen;

c) ha a személyes adatokat az Érintettel való kapcsolattartás céljára használják, legalább az Érintettel való első kapcsolatfelvétel alkalmával;

d) ha az Adatkezelési Tájékoztatóban szereplőn kívül más címzettel is közlik az adatokat, akkor legkésőbb az ilyen címzettel történő első közléskor;

e) ha a megszerzés céljától eltérő – azaz az Adatkezelési Tájékoztatóban eredetileg nem szereplő – adatkezelést is kíván végezni az Adatkezelő, akkor a további adatkezelést megelőzően.

2.2.3. Az Érintett hozzáférési joga (GDPR 15. cikk)

67) Az Érintett kérelmezheti a rá vonatkozó személyes adatokhoz való hozzáférést. Az Érintett jogosult arra, hogy kérelmére az Adatkezelőtől visszajelzést kapjon arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e, és ha ilyen adatkezelés folyamatban van, akkor jogosult arra, hogy hozzáférést kapjon a személyes adatokhoz és az alábbi információkhoz:

a) az adatkezelés céljai;

b) a személyes adatok kategóriái;

c) azon címzettek vagy címzettek kategóriái, akikkel, illetve amelyekkel a személyes adatokat közölték vagy közölni fogják, ideértve különösen a harmadik országbeli címzetteket, illetve a nemzetközi szervezeteket;

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

e) információ az Érintett azon jogáról, hogy kérelmezheti a Társaságtól a rá vonatkozó személyes adatok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen;

f) információ a Felügyeleti Hatósághoz (NAIH) címzett panasz benyújtásának jogáról;

g) ha az adatokat nem az Érintettől gyűjtötték, a forrásukra vonatkozó minden elérhető információ;

h) az automatizált döntéshozatal ténye, ideértve a profilalkotást is, valamint az alkalmazott logikára, illetve az ilyen adatkezelés jelentőségére és az Érintettre nézve várható következményeire vonatkozó információk.

68) Ha személyes adatoknak harmadik országba vagy nemzetközi szervezet részére történő továbbítására kerül sor, az Érintett jogosult továbbá arra is, hogy tájékoztatást kapjon a továbbításra vonatkozóan a jogszabály által előírt (GDPR 46. cikk) megfelelő garanciákról.

69) Az Érintett jogosult arra, hogy a személyes adatok másolatát kérje az Adatkezelőtől. Az Érintett által kért további másolatokért az Adatkezelő 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.

70) A másolat igénylésére vonatkozó jog nem érintheti hátrányosan mások jogait és szabadságait.

71) A személyes adat másolata a foglalkoztatási jogviszonyokra illetőleg az ügyfélkapcsolattal összefüggő jogviszonyokra vonatkozóan az azt tartalmazó nyilvántartásban tárolt személyes adatok másolatát jelenti, nem pedig a személyes adat (Adatkezelési Nyilvántartásban és Tájékoztatóban meghatározott célból történő) felhasználásával készült irat vagy bármely – akár elektronikus – dokumentum másolatát.

2.2.4. Helyesbítéshez való jog (GDPR 16. cikk)

72) Az Érintett erre vonatkozó kérelme esetén az Adatkezelő köteles indokolatlan késedelem nélkül helyesbíteni a rá vonatkozó pontatlan személyes adatokat. Figyelembe véve az adatkezelés célját, az Érintett jogosult arra, hogy kérje a hiányos személyes adatok – egyebek mellett kiegészítő nyilatkozat útján történő – kiegészítését.

73) Az Adatkezelő minden olyan címzettet tájékoztat a helyesbítésről, akivel, illetve amellyel a személyes adatot közölték, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel. Az Érintettet kérésére az Adatkezelő tájékoztatja e címzettekről.

2.2.5. Törléshez való jog (GDPR 17. cikk)

74) Az Érintett jogosult arra, hogy az Adatkezelőtől a rá vonatkozó személyes adatok törlését kérje, az Adatkezelő pedig köteles arra, hogy az Érintettre vonatkozó személyes adatokat indokolatlan késedelem nélkül törölje, ha az alábbi indokok valamelyike fennáll:

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

b) ha az Érintett – akár a kérelemmel egyidejűleg akár attól független formában – visszavonja az adatkezelés alapját képező hozzájárulását, és az adatkezelésnek nincs más jogalapja;

c) ha az Érintett tiltakozik a közérdekből, közhatalmi jogosítvány gyakorlása érdekében vagy a jogos érdekből történő adatkezelés ellen, és nincs elsőbbséget élvező jogszerű ok az adatkezelésre;

d) ha az Érintett tiltakozik a közvetlen üzletszerzés érdekében történő adatkezelés ellen az Adatkezelési Nyilvántartásban direkt marketing célként megjelölt tevékenység esetén;

e) ha a személyes adatokat jogellenesen kezelték;

f) ha a személyes adatokat az Adatkezelőre alkalmazandó uniós vagy hazai jogban előírt jogi kötelezettség teljesítéséhez törölni kell;

g) ha a személyes adatok gyűjtésére gyermekek számára nyújtott információs társadalommal összefüggő szolgáltatások kínálásával kapcsolatosan került sor.

75) Az Adatkezelő minden olyan címzettet tájékoztat a törlésről e személyes adatok másolatának, másodpéldányának törlése érdekében, akivel, illetve amellyel a személyes adatot közölték, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel. Az Érintettet kérésére az Adatkezelő tájékoztatja őt ezen címzettekről.

76) Az Érintett törlési jogának korlátozására csak a GDPR-ban írt alábbi kivételek fennállása esetén kerülhet sor, azaz a fenti indokok fennállása esetén a személyes adatok további megőrzése jogszerűnek tekinthető az alábbi esetekben:

a) ha a véleménynyilvánítás és a tájékozódás szabadságához való jog gyakorlása, vagy

b) ha valamely jogi kötelezettségnek való megfelelés, vagy

c) ha közérdekből végzett feladat végrehajtása, vagy

d) ha az Adatkezelőre ruházott közhatalmi jogosítvány gyakorlása miatt, vagy

e) ha népegészségügy területét érintő közérdekből,

f) ha közérdekű archiválás céljából, vagy

g) ha tudományos és történelmi kutatás céljából vagy statisztikai célból, vagy

h) ha jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez szükséges.

2.2.6. Az adatkezelés korlátozásához való jog (GDPR 18. cikk)

77) Az Érintett kérelmére az Adatkezelő korlátozza az adatkezelést, ha:

a) az Érintett vitatja a személyes adatok pontosságát, amely esetben a korlátozás arra az időtartamra vonatkozik, amely lehetővé teszi, hogy az Adatkezelő ellenőrizze a személyes adatok pontosságát;

b) az adatkezelés jogellenes, és az Érintett ellenzi az adatok törlését, és ehelyett kéri azok felhasználásának korlátozását;

c) az Adatkezelőnek már nincs szüksége a személyes adatokra adatkezelés céljából, de az Érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez;

d) az Érintett jogos érdek vagy közérdek jogalap alapján végzett adatkezelés ellen tiltakozott; amely esetben a korlátozás arra az időtartamra vonatkozik, amíg megállapításra nem kerül, hogy az Adatkezelő jogos indokai elsőbbséget élveznek-e az Érintett jogos indokaival szemben.

78) Ha az adatkezelés a fentiek alapján korlátozás alá esik, az ilyen személyes adatokat a tárolás kivételével csak az alábbi esetekben lehet kezelni:

a) az Érintett hozzájárulásával, vagy

b) jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez, vagy

c) más természetes vagy jogi személy jogainak védelme érdekében, vagy

d) az Európai Unió, illetve valamely tagállam fontos közérdekéből.

79) Az Adatkezelő köteles a korlátozás feloldásáról a feloldást megelőzően tájékoztatni az Érintettet, akinek kérése alapján az adatkezelés korlátozásra került.

80) Az Adatkezelő minden olyan címzettet tájékoztat, akivel, illetve amellyel a személyes adatot közölték, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel. Az Érintettet kérésére az Adatkezelő tájékoztatja ezen címzettekről.

2.2.7. Az adathordozhatósághoz való jog (GDPR 20. cikk)

81) Az Érintett jogosult arra, hogy a rá vonatkozó, általa az Adatkezelő rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja, továbbá jogosult arra, hogy ezeket az adatokat egy másik Adatkezelőnek továbbítsa anélkül, hogy ezt akadályozná az az Adatkezelő, amelynek a személyes adatokat a rendelkezésére bocsátotta, ha

a) az adatkezelés automatizált módon történik és

b) az adatkezelés jogalapja az Érintett hozzájárulása, vagy az Érintettel kötött szerződés teljesítése.

82) Az adatok hordozhatóságához való jog gyakorlása során az Érintett jogosult arra, hogy – ha ez technikailag megvalósítható – kérje a személyes adatok adatkezelők közötti közvetlen továbbítását.

83) Az adathordozhatóság jogának gyakorlása nem sértheti a törléshez való jogot. Az adathordozhatóság joga nem alkalmazandó abban az esetben, ha az adatkezelés közérdekű vagy az Adatkezelőre ruházott közhatalmi jogosítványai gyakorlásának keretében végzett feladat végrehajtásához szükséges.

84) Az adatok hordozhatóságához való jog nem érintheti hátrányosan mások jogait és szabadságait. A személyes adat hordozhatóságára vonatkozó jog a foglalkoztatási jogviszonyokra illetőleg az ügyfélkapcsolattal összefüggő jogviszonyokra vonatkozóan a nyilvántartásban tárolt személyes adatok hordozhatóságát (másolatát) jelenti, nem pedig a személyes adat – Adatkezelési Nyilvántartásban és Adatkezelési Tájékoztatóban meghatározott célból történő - felhasználásával készült irat vagy bármely – akár elektronikus – dokumentum hordozhatóságát (másolatát).

85) Az adatok hordozhatóságához való jog gyakorlása során az Adatfeldolgozó köteles együttműködni az Adatkezelővel, különösen az automatizált módon tárolt adatokra vonatkozó adathordozhatóság informatikai/technikai megvalósításában.

2.2.8. A tiltakozáshoz való jog (GDPR 21. cikk)

86) Az Érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból bármikor tiltakozzon személyes adatainak közérdekből, közhatalmi jogosítvány gyakorlása érdekében továbbá az Adatkezelő vagy harmadik fél jogos érdekében történő kezelése ellen, ideértve az ezeken alapuló profilalkotást is.

87) Az Érintett tiltakozása esetén az Adatkezelő a személyes adatokat nem kezelheti tovább, azaz törölni köteles, kivéve, ha az Adatkezelő bizonyítja, hogy az adatkezelést olyan kényszerítő erejű jogos okok indokolják, amelyek elsőbbséget élveznek az Érintett érdekeivel, jogaival és szabadságaival szemben, vagy amelyek jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódnak.

88) Ha a személyes adatok kezelése közvetlen üzletszerzés érdekében történik (az Adatkezelési Nyilvántartásban direkt marketing célként megjelölt tevékenység esetén), az Érintett jogosult arra, hogy bármikor tiltakozzon a rá vonatkozó személyes adatok e célból történő kezelése ellen, ideértve a profilalkotást is, amennyiben az a közvetlen üzletszerzéshez kapcsolódik.

89) Ha az Érintett tiltakozik a személyes adatok közvetlen üzletszerzés érdekében történő kezelése ellen, akkor a személyes adatok a továbbiakban e célból nem kezelhetők, azaz törlendők.

90) A tiltakozáshoz való jogra legkésőbb az Érintettel való első kapcsolatfelvétel során kifejezetten fel kell hívni a figyelmet, és az erre vonatkozó tájékoztatást egyértelműen és minden más információtól elkülönítve kell megjeleníteni a Tájékoztató mintájával összhangban.

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

92) Az Érintett jogosult arra, hogy személyes adatainak kezeléséhez adott hozzájárulását bármely időpontban visszavonja. A hozzájárulás visszavonása nem érinti a hozzájáruláson

alapuló, a visszavonás előtti adatkezelés jogszerűségét. A hozzájárulás visszavonását az Érintett ugyanolyan egyszerű módon jogosult megtenni, mint annak megadását.

2.2.8.1. Automatizált döntéshozatal, profilalkotás

93) Az Adatkezelő csak akkor alkalmaz kizárólag automatizált adatkezelésen – ideértve a profilalkotást is – alapuló olyan döntést, amely az Érintettre nézve joghatással jár vagy őt hasonlóképpen jelentős mértékben érinti, ha az Adatkezelési Nyilvántartásban rögzített alábbi három jogalap szerinti tevékenységre vonatkozik:

a) az Adatkezelő és az Érintett közötti szerződés megkötése vagy teljesítése érdekében szükséges;

b) meghozatalát az Adatkezelőre alkalmazandó olyan uniós vagy hazai jogszabály teszi lehetővé, amely az Érintett jogainak és szabadságainak, valamint jogos érdekeinek védelmét szolgáló megfelelő intézkedéseket is megállapít;

c) az Érintett kifejezett hozzájárulásán alapul.

94) Az automatizált döntéshozatalra és a profilalkotás további követelményeire a GDPR alkalmazandó.

2.2.9. Az Érintetti kérelemmel és teljesítésével kapcsolatos előírások

95) A Társaság köteles elősegíteni az Érintettek jogainak gyakorlását.

96) Az Érintett a 2.2.2 pont szerinti jogainak gyakorlásával kapcsolatos kérelmét jogosult elektronikus úton benyújtani a BKK online bejelentő felületén, a bkk@bkk.hu, vagy közvetlenül az adatvedelem@bkk.hu e-mail címen, illetve szóban és írásban bármelyik BKK Ügyfélközpontban, vagy postai úton a BKK-nak címzett küldeményben (1075 Budapest, Rumbach Sebestyén utca 19-21., 1241 Budapest, Pf. 200.)

97) A szóban előterjesztett kérelemről jegyzőkönyvet kell felvenni. A jegyzőkönyv felvételekor vagy az írásbeli kérelem átvételekor szükséges az Érintett azonosítása, mely személyazonosításra alkalmas hatósági igazolvány bemutatásával történik. A megtekintett igazolvány másolása tilos. A kérelemre az ügyintézőnek rá kell vezetni az azonosítás megtörténtét.

98) Az Adatkezelő az Érintett jogainak gyakorlására irányuló kérelem teljesítését nem tagadhatja meg, kivéve, ha bizonyítja, hogy az Érintettet nem áll módjában azonosítani.

99) A kérelem benyújtását és dokumentált érkeztetését követően az Adatkezelőhaladéktalanul köteles megvizsgálni a kérelmet az alábbiak szerint:

a) az arra jogosult Érintett nyújtotta-e be a kérelmet,

b) a kérelem melyik érintetti jog gyakorlására vonatkozik,

c) a kérelemben foglaltak teljesítésére vonatkozó intézkedés megtételére az Adatkezelő jogszabály szerint kötelezett-e.

100) Amennyiben az Adatkezelőnek megalapozott kétségei vannak a kérelmet benyújtó természetes személy kilétével kapcsolatban, és az Adatkezelő bizonyítani tudja, hogy nincs abban a helyzetben, hogy azonosítsa az Érintettet, további, az Érintett személyazonosságának megerősítéséhez szükséges információk benyújtását kérheti.

101) A kérelem vizsgálatát követően az Ügyfélszolgálat Osztály – amennyiben szükséges, az ügyben érintett szervezeti egységek bevonásával – elkészíti a válasz tervezetét, melyet mérlegelést követően, a kérelem összetettségére tekintettel, szükség esetén véleményezésre vagy jóváhagyásra megküld a Compliance Osztály részére.

102) Az Adatkezelő díjmentesen és indokolatlan késedelem nélkül, de legkésőbb a kérelem beérkezésétől számított egy hónapon belül visszajelzést ad az Érintett számára az alábbiakról:

a) intézkedés megtételéről vagy

b) az intézkedés elmaradásáról

c) az intézkedés elmaradásának (ideértve a határidő meghosszabbítást is) jogszabály szerinti okairól,

d) arról, hogy az Érintett panaszt nyújthat be a NAIH-nál és élhet bírósági jogorvoslati jogával,

e) ha további kiegészítő információ megadása vált szükségessé a kérelemmel összefüggő azonosítás céljából és az Adatkezelő bármely oknál fogva kezeli az Érintett ilyen kiegészítő személyes adatait, akkor az erre vonatkozó tájékoztatásról.

103) Amennyiben feltétlenül szükséges és indokolt, a válaszadásra nyitva álló egy hónapos határidő további két hónappal meghosszabbítható, figyelembe véve a kérelem összetettségét és a kérelmek számát.

104) Szükség esetén a visszajelzéssel egyidejűleg kell értesíteni a címzetteket is.

105) A kérelem alapján történő intézkedés kizárólag akkor tagadható meg, vagy kizárólag akkor számítható fel ésszerű összegű díj a kért információra, illetve az intézkedés meghozatalával járó adminisztratív költségekre is figyelemmel, ha az Adatkezelő bizonyítani tudja, hogy a kérelem egyértelműen megalapozatlan vagy – különösen ismétlődő jellege miatt – túlzó.

106) Ha az Adatkezelő nem tesz intézkedést az Érintett megkeresése alapján, akkor késedelem nélkül, de legkésőbb 1 hónapos határidőn belül tájékoztatja az Érintettet az intézkedés elmaradásának, a kérelem teljesítése megtagadásának okairól.

107) A kérelemre történő visszajelzés mintáját a jelen szabályzat 6. számú melléklete tartalmazza, a címzetti értesítések mintáját a jelen szabályzat 7. számú melléklete tartalmazza.

108) Ha az Érintett elektronikus úton nyújtotta be a megkeresést, akkor a választ az Adatkezelő lehetőség szerint elektronikus úton adja meg, kivéve, ha az Érintett azt másként kéri.

109) A Compliance Osztály – az Ügyfélszolgálat Osztály bevonásával – évente, a tárgyév végét követő január 31-ig jelentést, statisztikai adatszolgáltatást küld a DPO számára a Társaság vonatkozásában tárgyévben előforduló kérelmekről és címzetti értesítésekről. A jelentés tartalmazza a kérelmek számát érintetti jogonkénti bontásban, és a megtett intézkedéseket.

2.3. Adatvédelmi szereplők és feladataik

2.3.1. Az Adatvédelmi tisztviselő (DPO) kijelölése és feladatai

110) Az BKK Zrt. Adatvédelmi tisztviselőjét a Társaság vezérigazgatója bízza meg, vagy nevezi ki.

111) Az Adatvédelmi tisztviselő a Társaság munkavállalójaként, vagy megbízási szerződés keretében láthatja el a feladatait. Kinevezése, megbízása során a szakmai rátermettség és különösen az adatvédelmi jog és gyakorlat szakértői szintű ismerete, valamint a GDPR 39. cikkében említett feladatok ellátására való alkalmasságra szükséges figyelemmel lenni.

112) A kinevezést, megbízást követően a Társaság honlapján közzéteszi az Adatvédelmi tisztviselő elérhetőségét. A Társaság az adatvédelmi tisztviselő nevét és elérhetőségét közli a Felügyeleti Hatósággal (NAIH).

113) Az Adatvédelmi tisztviselő ellátja a GDPR és az Info tv. által nevesített feladatokat, e tekintetben köteles szorosan együttműködni a Társaság szervezeti egységeivel, vezető tisztségviselőivel.

114) Az Adatvédelmi tisztviselő feladatai különösen:

a) tájékoztatást, állásfoglalást és szakmai tanácsot ad az Adatkezelő részére a GDPR valamint egyéb uniós vagy hazai adatvédelmi rendelkezések szerinti kötelezettségeikkel kapcsolatban;

b) ellenőrzi a GDPR-nak, továbbá egyéb uniós vagy hazai szabályozásoknak, rendelkezéseknek, a jelen szabályzatnak és az adatvédelemmel összefüggő egyéb belső szabályozásnak történő megfelelést;

c) felelős a jelen szabályzat és annak részét képező mintadokumentumok, formanyomtatványok és mellékletek véleményezéséért és jóváhagyásáért;

d) a kezdetektől részt vesz a Társaság induló – személyes adatkezelésekkel járó – projektjeiben, azokat adatvédelmi szempontból támogatja;

e) szakmai támogatást nyújt az Adatkezelő Adatkezelési Nyilvántartásának elkészítéséhez és naprakészen tartásához;

f) részt vesz az adatvédelmi incidensek kivizsgálásában, szakmai iránymutatást ad a szükséges intézkedések megtételére, valamint szükség esetén az adatvédelmi incidenst bejelenti a NAIH felé;

g) részt vesz a Társaság adatvédelemmel kapcsolatos belső audit tevékenységében;

h) szakmai támogatást nyújt és javaslatot tesz a BKK személyes adatvédelemmel kapcsolatos szabályozására, annak módosításra;

i) közreműködik a személyes adatkezelési műveletekben részt vevő munkavállalók tudatosság-növelésében és képzésében;

j) az Adatkezelő kérésére szakmai tanácsot ad az adatvédelmi hatásvizsgálatokra, érdekmérlegelésekre, továbbá adatfeldolgozói vagy adatkezelői megállapodások megkötésére vonatkozóan, valamint nyomon követi azok elvégzését, az elkészült dokumentumokat jóváhagyja;

k) az Adatkezelő kérésére bármely adatvédelmi érintettségű kérdésben állásfoglalást ad;

l) együttműködik és bármely kérdésben konzultációt folytat a Felügyeleti Hatósággal, kapcsolattartási pontként szolgál a NAIH felé.

115) Az Adatvédelmi tisztviselő a személyes adatok védelmével kapcsolatos összes ügybe megfelelő módon és időben bekapcsolódhat, a személyes adatokhoz és az adatkezelési műveletekhez minden esetben hozzáférhet.

116) Az Adatvédelmi tisztviselőt feladatai ellátása során jogszabályban meghatározott titoktartási kötelezettség, valamint az adatok bizalmas kezelésére vonatkozó kötelezettség köti.

117) Az Adatvédelmi tisztviselő a feladatai ellátásával kapcsolatban utasításokat senkitől sem fogadhat el.

118) Az Adatvédelmi tisztviselő jelen szabályzatba foglaltakon felül egyéb – munkaszerződésében vagy megbízási szerződésében rögzített - feladatokat is elláthat.

2.3.2. A Compliance Osztály adatvédelmi feladatai

119) A Compliance Osztály feladata a külső-belső adatvédelmi és adatkezelési követelményeknek, adatvédelmi szempontoknak való megfelelés elősegítése, koordinációja, nyomon követése.

120) Kapcsolattartói feladatot lát el és szorosan együttműködik a Társaság Adatvédelmi tisztviselőjével, valamint az Adatkezelésért felelős szervezeti egységekkel, továbbá az általuk biztosított és továbbított információk alapján vezeti a személyes adatok kezelésével összefüggésben készített nyilvántartásokat (ideértve: Adatkezelési Nyilvántartás, Adatvédelmi incidensek nyilvántartása).

121) A Compliance Osztály operatív módon közreműködik a Társaság adatvédelmi megfelelőségének biztosításában, ennek keretében:

a) ellenőrzi a GDPR, az Info tv., valamint a személyes adatkezelésre vonatkozó más jogszabályok, a belső adatvédelmi és adatbiztonsági szabályozások kapcsolódó rendelkezéseinek és követelményeknek a megtartását;

b) valamennyi szervezeti egységnél jogosult betekinteni a személyes adatkezelési folyamatokba, valamint a kapcsolódó dokumentumokba;

c) az Adatkezelésért felelős szervezeti egység által biztosított információk és előkészített dokumentum tervezetek alapján – szükség szerint a DPO bevonásával és jóváhagyása mellett – véglegesíti az Adatkezelési Tájékoztatókat, adatvédelmi hatásvizsgálatokat, érdekmérlegelési teszteket, valamint az adatfeldolgozói megállapodásokat;

d) a kezdetektől a DPO-val együtt részt vesz a Társaság induló – személyes adatkezelésekkel járó - projektjeiben, azokat adatvédelmi szempontból támogatja;

e) az Adatkezelésért felelős szervezeti egység, az Adatvédelmi koordinátor kérésére bármely – nem a DPO hatáskörébe tartozó – adatvédelmi érintettségű kérdésben állásfoglalást, szakmai tanácsot ad;

f) amennyiben a DPO nem a BKK munkavállalója, úgy kivizsgálja – szükség esetén a DPO egyidejű tájékoztatásával és bevonásával – a hozzá érkező bejelentéseket, jogosulatlan adatkezelés és törvénysértés észlelése esetén annak megszüntetésére javaslatot tesz; szükség esetén segítséget nyújt a törvényes állapot helyreállításához.

2.3.3. Adatkezelésért felelős szervezeti egység és az Adatvédelmi koordinátor

122) Az Adatkezelésért felelős szervezeti egység – különösen jogszabály változás, új belső folyamatok, fejlesztések, projektek, vagy új szolgáltatások bevezetése esetén – köteles a személyes adatok kezelésével bármely módon összefüggő tervezett tevékenységet a tevékenység megkezdését megelőző kellő időben bejelenteni az Adatvédelmi koordinátoron keresztül a Compliance Osztálynak az adatvedelem@bkk.hu e-mail címen.

123) Az Adatkezelésért felelős szervezeti egységnek – a mintadokumentumok megfelelő szintű előkészítésén felül – minden esetben meg kell adnia az adatvédelmi koncepció kidolgozásához szükséges minden releváns információt a Compliance Osztály és a DPO részére a jelen szabályzat 11. számú mellékletében szereplő Igényfelmérő kérdőív kitöltésével. A DPO és a Compliance Osztály a szükséges adatvédelmi dokumentumokat kizárólag az összes – adatkezelés szempontjából lényeges – információ birtokában tudja véglegesíteni és jóváhagyni.

124) Az adatkezelés kizárólag az összes adatvédelmi dokumentum elkészültét és a DPO vagy a Compliance Osztály jóváhagyását követően kezdhető meg.

125) Az Adatvédelmi koordinátor:

a) közreműködik, az adott Adatkezelésért felelős szervezeti egységet érintő adatkezeléssel összefüggő döntések előkészítésében, valamint az érintettek jogainak biztosításában;

b) közreműködik és koordinálja a jelen szabályzat által biztosított formanyomtatványok és minták alapján az adott Adatkezelésért felelős szervezeti egység adatvédelmi tárgyú dokumentumainak – különösen az érdekmérlegelési tesztek, szerződések, megállapodások, szabályozások és adatkezelési tájékoztatók, valamint az adatvédelmi hatásvizsgálatok – előkészítését és kidolgozását, valamint továbbítja azokat a Compliance Osztály részére ellenőrzésre és jóváhagyásra;

c) az egyes adatkezelési célokkal összefüggésben felelős szervezeti egységén belül az Adatkezelési Nyilvántartás naprakészen tartásához – jelen szabályzat 2.4.1 pontjában foglaltak szerint – információt biztosít a Compliance Osztály részére.

d) figyelemmel kíséri az adott szakterület adatkezelési tevékenységét, és bármilyen új adatkezelési tevékenység, vagy észlelt rendellenesség gyanúja esetén haladéktalanul tájékoztatja a Compliance Osztályt az adatvedelem@bkk.hu e-mail címen.

126) Az Adatvédelmi koordinátort az Adatkezelésért felelős szervezeti egységnek be kell vonni a saját szakterületét érintő összes adatvédelmi témájú ügybe.

2.3.4. Kapcsolattartás az Adatvédelmi tisztviselővel és az adatvédelmi koordinátorral

127) Adatvédelmi kérdésekben a Compliance osztállyal történő operatív kapcsolattartás, valamint az adatkezelési tevékenységek társaságon belüli megfelelő koordinálása céljából és érdekében valamennyi szervezeti egység vezetője – lehetőség szerint Osztály szinten - Adatvédelmi koordinátort jelöl ki, akinek nevét legkésőbb jelen Szabályzat hatályba lépését követő 1 (egy) héten belül megküldi a Compliance Osztály részére, aki arról nyilvántartást készít.

128) Amennyiben a Társaság bármely munkavállalója a Társaság működése körében személyes adatkezeléssel összefüggően intézkedést igénylő körülményt észlel, az alábbiak szerint kell eljárnia:

a) Ha valamely Érintett személyes adatkezeléssel kapcsolatos kérelmet juttat el hozzá vagy a Társasághoz, haladéktalanul köteles értesíteni az Adatvédelmi koordinátort.

b) Ha adatvédelmi incidensre utaló eseményt tapasztal vagy ezzel kapcsolatban bármely más releváns információhoz jut, haladéktalanul köteles értesíteni a Compliance Osztályt és köteles továbbítani neki az összes rendelkezésére álló releváns dokumentumot, információt.

c) Bármilyen adatvédelmi érintettségű rendellenesség észlelése esetén haladéktalanul jelzi azt a Compliance Osztálynak.

129) Amennyiben a DPO nem a BKK munkavállalója, a Compliance Osztály látja el a kapcsolattartói és koordinációs feladatokat a Társaság és a DPO között, az Adatvédelmi tisztviselő részére továbbítja az Adatkezelésért felelős szervezeti egység által előkészített dokumentumokat, illetve felügyeli és nyilvántartja a személyes adatkezeléssel kapcsolatos munkavégzést.

130) Az adatvédelmi feladatoknak a 3 szint közötti megosztását az alábbi táblázat mutatja be:

Feladat típusok	**Adatvédelmi tisztviselő feladatai**	**Compliance Osztály feladatai**	**Adatvédelmi koordinátor/Adatkezelésért felelős szervezeti egység feladatai**
Proaktív tanácsadás, támogatás, tájékoztatás adatvédelmi kérdésekről	Végső szakmai tanácsadás, iránymutatás, javaslat	Szakmai tanácsadás, iránymutatás, javaslat	Operatív feladatok ellátása, probléma, kérdés esetén a Compliance Osztályhoz fordulás lehetőségével
Projekttámogatás	Proaktív tanácsadás, iránymutatás, javaslattétel	Kapcsolattartás, koordináció, iránymutatás, javaslattétel, szakmai anyagok véglegesítése	A projekttel kapcsolatos minden releváns információ megküldése a Compliance Osztály felé. Szakmai anyagok (pl. adatkezelési tájékoztató, érdekmérlegelési teszt) előkészítése.
Adatvédelmi szabályok betartása	Ellenőrzés	Szakmai tanácsadás, iránymutatás, állásfoglalás, javaslattétel	Adatszolgáltatás

Feladat típusok	**Adatvédelmi tisztviselő feladatai**	**Compliance Osztály feladatai**	**Adatvédelmi koordinátor/Adatkezelésért felelős szervezeti egység feladatai**
Hatásvizsgálatok, érdekmérlegelések	Szakmai tanácsadás, nyomon követés, jóváhagyás	Támogatás, iránymutatás, javaslattétel, véglegesítés	Előkészítés a mintadokumentumok alapján, adatszolgáltatás
Adatkezelési nyilvántartás kezelése	Mintát ad, standardizál, ellenőriz	Nyilvántartás vezetése, kezelése	Adatszolgáltatás a szervezeti egység adatkezeléseiről
Adatkezelési Tájékoztatók elkészítése	Mintát ad, igény szerint véleményez, ellenőriz	Szakmai tanácsadás, iránymutatás, javaslattétel, véglegesítés	Adatszolgáltatás a szervezeti egység adatkezeléseiről, előkészítés a mintadokumentum alapján
NAIH kapcsolattartás, együttműködés	Kizárólagosan tartja a Felügyeleti Hatósággal a kapcsolatot		
Érintetti kérelmek, bejelentések kezelése	Szükség esetén iránymutatás a kivizsgáláshoz, összetett ügyek esetén véleményezés,	Szükség esetén iránymutatás, véleményezés, DPO-val egyeztetés	Bejelentések fogadása, továbbítás az Ügyfélszolgálat Osztály részére, közreműködés a kivizsgálásban,

Feladat típusok	**Adatvédelmi tisztviselő feladatai**	**Compliance Osztály feladatai**	**Adatvédelmi koordinátor/Adatkezelésért felelős szervezeti egység feladatai**
	választerv jóváhagyása		válaszadásban, szükséges intézkedések megtétele, probléma, kérdés esetén a Compliance Osztályhoz fordulás lehetőségével
Adatvédelmi oktatások	Oktatási anyag szakmai előkészítése, oktatás	Oktatási anyag szakmai előkészítése, oktatás	Részvétel az oktatásokon
Incidenskezelés	Incidens kivizsgálás koordinálása, kockázatértékelés, döntési javaslat a Vezérigazgató részére, incidens bejelentése a NAIH-hoz, amennyiben szükséges	Szakmai tanácsadás, iránymutatás, javaslattétel, közreműködés a kivizsgálásban, nyilvántartás kezelése, szükség esetén gondoskodik az érintetti tájékoztatás előkészítéséről.	Információgyűjtés, adatszolgáltatás, közreműködés a kivizsgálásban, szükséges intézkedések megtétele
Beszámolás	Éves beszámoló összeállítása	Negyedéves státuszjelentések	Információ, / adatszolgáltatás

2.4. Az adatkezelési tevékenységekkel kapcsolatos kötelező nyilvántartások

2.4.1. Adatkezelési Nyilvántartás vezetése és felülvizsgálata, a törlési kötelezettség

131) Az Adatkezelő az általa végzett adatkezelési tevékenységekről elektronikus nyilvántartási rendszerben nyilvántartást vezet a GDPR 30. cikke alapján.

132) Az Adatkezelési Nyilvántartás tartalmát naprakészen kell tartani és rendszeresen – szükség szerint, de legalább évente – felül kell vizsgálni. Ennek keretében rögzíteni kell az új adatkezelési tevékenységeket, különösen új adatkezelési cél vagy új érintetti kör esetén.

133) A nyilvántartásból törölni kell a már nem végzett adatkezelési tevékenységeket. Az Adatvédelmi koordinátor az adatvedelem@bkk.hu e-mailre küldött elektronikus levélben jelzi, hogy mely adatkezelési tevékenység, milyen okból szűnt meg, valamint kéri az adatkezelési tevékenység Adatkezelési Nyilvántartásból való törlését.

134) A törlést az Adatkezelési Nyilvántartásból az Adatvédelmi koordinátor kérelmére a Compliance Osztály végzi el

135) Az Adatkezelési Nyilvántartás frissítésével egyidejűleg frissíteni szükséges a vonatkozó Adatkezelési Tájékoztatókat is, amelyek alapján szükség szerint ismételten tájékoztatni kell az Érintetteket.

136) Az Adatvédelmi koordinátor az adatvedelem@bkk.hu e-mailre küldött elektronikus levélben jelzi, hogy mely adatkezelési tevékenység, milyen okból és milyen módon változott, valamint kéri az adatkezelési tevékenység Adatkezelési Nyilvántartásban történő módosítását.

137) A módosítást az Adatkezelési Nyilvántartásban a Compliance Osztály végzi el.

138) Az Adatkezelési tevékenységért felelős szervezeti egység a beépített és alapértelmezett adatvédelem elvét figyelembe véve különösen jogszabály változás, új belső folyamatok, fejlesztések, projektek, vagy szolgáltatások esetén köteles a személyes adatokkal bármely módon összefüggő tervezett tevékenységeket az Adatkezelési Nyilvántartásban rögzítendő adatok megadásával – különös tekintettel az adatkezelés céljára, az érintetti körre, az adat tárolásának helyére, az igénybe vett Adatfeldolgozóra, címzettek , valamint a kezelni kívánt személyes adatok körére - a tevékenység megkezdését megelőzően bejelenteni az Adatvédelmi koordinátoron keresztük a Compliance Osztálynak az adatvedelem@bkk.hu e-mail címen.

139) A Compliance Osztály az új adatkezelési tevékenységet – szükség esetén a DPO szakmai javaslata mellett – felviszi az Adatkezelési Nyilvántartásba, majd az alapján – az Adatkezelésért felelős szervezeti egység előkészítését és közreműködését követően –

elkészíti az adatkezelés megkezdéséhez szükséges dokumentumokat (adatvédelmi hatásvizsgálat, érdekmérlegelési teszt, adatkezelési tájékoztató).

140) Az Adatkezelő az Adatkezelési Nyilvántartásban rögzített, a személyes adatok kezelésére vonatkozó jogszerű időtartam elteltét követően a személyes adatot törölni köteles.

141) Annak biztosítása érdekében, hogy a személyes adatok tárolása a szükséges időtartamra korlátozódjon, az Adatkezelési tevékenységért felelős szervezeti egység rendszeresen felülvizsgálja az általa kezelt személyes adatokat az alábbiak szerint:

a) ***naponta***, amennyiben az Adatkezelési Nyilvántartás a vonatkozó adatkezelési cél tekintetében napokban meghatározott időtartamot rögzít;

b) ***havonta***, amennyiben az Adatkezelési Nyilvántartás a vonatkozó adatkezelési cél tekintetében hónapokban meghatározott időtartamot rögzít;

c) ***negyedévente***, amennyiben az Adatkezelési Nyilvántartás a vonatkozó adatkezelési cél tekintetében a munkaviszony vagy egyéb jogviszony végét rögzíti;

d) ***negyedévente,*** amennyiben az Adatkezelési Nyilvántartás a vonatkozó adatkezelési cél tekintetében az elévülési idővel összefüggő időtartamot rögzít;

e) ***a tárgyév végét megelőző negyedéves felülvizsgálat során***, amennyiben az Adatkezelési Nyilvántartás a vonatkozó adatkezelési cél tekintetében a tárgyév végét rögzíti.

2.4.2. Nyilvántartás az adatvédelmi incidensekről

142) Az adatkezelési tevékenységekkel összefüggő adatvédelmi incidensekről a Társaság Adatvédelmi tisztviselőjének szakmai iránymutatása alapján a Compliance Osztály vezet nyilvántartást a GDPR 33. cikk (5) bekezdése alapján, a jelen szabályzatban, valamint a Társaság mindekor hatályos ***Adatvédelmi incidenskezelés eljárásrendről szóló vezérigazgatói utasítás***ában foglaltaknak megfelelően, feltüntetve az adatvédelmi incidenshez kapcsolódó tényeket, annak hatásait és az orvoslására tett intézkedéseket.

143) Az adatvédelmi incidensek nyilvántartás mintáját jelen szabályzat 8. számú melléklete tartalmazza.

144) Az adatvédelmi incidens nyilvántartást folyamatosan naprakészen kell tartani. A nyilvántartás a hatósági bejelentési kötelezettség alá tartozó és a hatósági bejelentési kötelezettség alá nem tartozó adatvédelmi incidenseket is tartalmazza.

2.4.3. Az adatfeldolgozói nyilvántartás vezetése és felülvizsgálata

145) A BKK az Adatkezelési Nyilvántartás keretében nyilvántartást vezet az Adatkezelő nevében végzett adatkezelési tevékenységekről a GDPR 30. cikk (2) bekezdése alapján. Az

adatfeldolgozói nyilvántartást az alapjául szolgáló adatfeldolgozói megállapodások módosulása, megszűnése vagy új adatfeldolgozási megállapodás megkötésével egyidejűleg folyamatosan frissíteni kell.

2.5. Személyes adatok törlésére vonatkozó lényeges szempontok

146) Az Adatkezelő:

a) a 2.4.1 pont szerinti Adatkezelési Nyilvántartásban az egyes adatkezelési tevékenységek vonatkozásában, az adatkezelés célja tekintetében meghatározott időtartam elteltét, vagy

b) az 2.2.2 pont szerinti az Érintett törlésre irányuló kérelmének – törlési jog gyakorlása vagy tiltakozási jog gyakorlása – teljesítéséről szóló döntést követően

törölni vagy anonimizálni köteles a személyes adatot az alap adatbázisból papír alapon és elektronikus tárolási helyén is. A törlési, anonimizálási kötelezettség vonatkozik a személyes adatok másolataira is.

147) Az Adatkezelési tevékenységért felelős szervezeti egység folyamatosan nyomon követi az általa kezelt személyes adatokat és megőrzési időtartamokat, meghatározza a törlendő tételeket és intézkedik a törlés/anonimizálás tekintetében.

148) Az informatikai rendszerekből történő törlésekkel kapcsolatos előírásokat a mindenkor hatályos Információbiztonsági szabályzatban és az informatikai rendszerekre vonatkozó külön szabályzatokban szükséges rögzíteni.

2.6. Adatbiztonság

149) A GDPR 32. cikke értelmében az Adatkezelő és az Adatfeldolgozó a tudomány és technológia állására, a megvalósítás költségeire figyelemmel, valamint az adatkezelési tevékenységei természetes személyek jogaira és szabadságaira jelenlett kockázatait figyelembe véve megfelelő technikai és szervezési intézkedéseket hajt végre annak érdekében, hogy a kockázat mértékének megfelelő, azzal arányos védelmi intézkedések útján a megfelelő szintű adatbiztonságot garantálja.

150) Az Adatkezelő és az Adatfeldolgozó egyúttal biztosítja, hogy a személyes adatokhoz hozzáféréssel rendelkező munkavállalói és közreműködői kizárólag a jogszabályoknak illetőleg a mindenkor hatályos információbiztonsági szabályzatban meghatározottaknak megfelelően kezeljék a személyes adatokat kivéve, ha ettől való eltérésre uniós vagy tagállami jog kötelezi őket.

151) Fentiek érdekében a mindenkor hatályos információbiztonsági szabályzatnak kell rögzítenie az alábbiakat:

a) a biztonság megfelelő szintjének meghatározását, figyelembe véve az adatkezelésből eredő olyan kockázatokat, amelyek a személyes adatok véletlen vagy jogellenes megsemmisítéséből, elvesztéséből, megváltoztatásából, jogosulatlan nyilvánosságra hozatalából vagy az azokhoz való jogosulatlan hozzáférésekből erednek;

b) fizikai vagy műszaki adatvédelmi incidens esetén az arra vonatkozó intézkedéseket, hogy a személyes adatokhoz való hozzáférését és az adatok rendelkezésre állását a kellő időben vissza lehessen állítani;

c) a személyes adatok kezelésére használt informatikai rendszerek és szolgáltatások folyamatos bizalmas jellegének, integritásának, rendelkezésre állásának és ellenálló képességének biztosítására vonatkozó előírásokat;

d) a személyes adatok lehetőség szerinti álnevesítésére vagy titkosítására vonatkozó előírásokat;

e) az adatkezelés biztonságának garantálására hozott intézkedések hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárásokat, többek között az adatokhoz történő hozzáférés visszakövethetőségére vonatkozó intézkedéseket;

f) adatok törlésére vonatkozó előírásokat és felelősségi köröket a jelen szabályzattal összhangban.

3. ZÁRÓ RENDELKEZÉSEK

152) A jelen Szabályzat a kihirdetés napján lép hatályba.

153) Jelen szabályzat hatályba lépésével egyidejűleg hatályát veszti a BKK Zrt. személyes adatkezelési és adatvédelmi szabályzatáról szóló 44/2023/VIG/CO/1. sz. Vezérigazgatói utasítás.

154) A Szabályzat elkészítéséért, továbbá rendszeres felülvizsgálatáért a Compliance Osztály vezetője a felelős.

Budapest, 2024. október 29.

Dr. Walter Katalin Irén s.k.
vezérigazgató
BKK Zrt.

4. MELLÉKLETEK

1. számú melléklet: Adatfeldolgozói megállapodás minta
2. számú melléklet: Hozzájáruló nyilatkozat minta
3. számú melléklet: Érdekmérlegelési teszt minta
4. számú melléklet: Adatvédelmi hatásvizsgálat módszertani és kitöltési útmutató
5. számú melléklet: Adatkezelési Tájékoztató minta
6. számú melléklet: Válaszlevél érintetti kérelemre minta
7. számú melléklet: Értesítés a címzetteknek minta
8. számú melléklet: Adatvédelmi incidensek nyilvántartása minta
9. számú melléklet: Útmutató informatikai eszközök és gépjárművek ellenőrzésének adatkezeléséhez
10. számú melléklet: Útmutató munkára alkalmas állapot ellenőrzésének adatkezelésére
11. számú melléklet: Igényfelmérő kérdőív