Államadósság Kezelő Központ Zártkörűen Működő Részvénytársaság

ADATVÉDELMI ÉS ADATKEZELÉSI SZABÁLYZAT

Tartalomjegyzék

1. ÁLTALÁNOS RENDELKEZÉSEK 3
1.1. A Szabályzat célja és tárgya 3
1.2. Az Adatkezelő személye és tevékenysége 4
1.3. A Szabályzat tárgyi hatálya 4
1.4. A Szabályzat alanyi hatálya 4
1.5. Fogalom meghatározások 4
2. ADATVÉDELMI ALAPELVEK 8
3. AZ ADATKEZELÉS JOGALAPJAI 10
4. AZ ADATKEZELÉSSEL KAPCSOLATOS RENDELKEZÉSEK 12
4.1. Adatállományok kezelése 12
4.2. A levéltári anyag kezelése 13
4.3. Az adatkezelés típusai 13
4.4. Az adatvédelem ÁKK Zrt.-n belüli szervezete 13
4.5. Adatbiztonság 15
4.6. Adatvédelmi hatásvizsgálat 19
5. ÉRINTETTEK JOGGYAKORLÁSÁNAK BELSŐ ELJÁRÁSRENDJE 20
5.1. Tájékoztatás és a személyes adatokhoz való hozzáférés joga 20
5.2. Törléshez (elfeledtetéshez) való jog 21
5.3. Az adatkezelés elleni tiltakozás kezelése 23
5.4. A kezelt adatok helyesbítéséhez, kiegészítéséhez való jog 23
5.5. Adatkezelés korlátozásához való jog 24
5.6. Adathordozhatósághoz való jog 24
6. ADATKEZELÉS TERVEZÉSE 25
7. ADATVÉDELMI INCIDENSEKKEL KAPCSOLATOS KÖTELEZETTSÉGEK ÉS RENDELKEZÉSEK 26
8. AZ ADATVÉDELMI TISZTVISELŐ/ADATVÉDELMI FELELŐS 26
9. ADATTOVÁBBÍTÁS 28
9.1. Általános rendelkezések 28
9.2. Adattovábbítás megkeresés alapján 28
10. ADATFELDOLGOZÓKRA VONATKOZÓ ÁLTALÁNOS RENDELKEZÉSEK 29
11. AZ ADATFELDOLGOZÓI SZERZŐDÉSEK KÖTELEZŐ TARTALMI ELEMEI 30
12. KÖZÉRDEKŰ ADATOK MEGISMERÉSÉRE IRÁNYULÓ IGÉNY ÉS TELJESÍTÉSE 32
13. SZEMÉLYZETI, BÉR- ÉS MUNKAÜGYI NYILVÁNTARTÁS 32
13.1. Személyügyi nyilvántartás 32
13.2. Bér- és munkaügyi nyilvántartás 33
14. E-MAIL FIÓK, INFORMATIKAI ESZKÖZ ÉS MOBILTELEFON HASZNÁLATÁNAK ELLENŐRZÉSÉVEL KAPCSOLATOS ADATKEZELÉS 34
14.1. E-mail fiók használatának ellenőrzésével kapcsolatos adatkezelés 34
14.2. Számítógép, hordozható számítógép, használatának ellenőrzésével kapcsolatos adatkezelés 35
14.3. Mobiltelefonok és tabletek használatának ellenőrzésével kapcsolatos adatkezelés 36
15. ADÓTITOK KÖRÉBE TARTOZÓ ADATOK KEZELÉSE ÉS VÉDELME 37
16. BANKTITOK KÖRÉBE TARTOZÓ ADATOK KEZELÉSE ÉS VÉDELME 37
17. ÉRTÉKPAPÍRTITOK KÖRÉBE TARTOZÓ ADATOK KEZELÉSE ÉS VÉDELME 37
18. A MINŐSÍTETT ADAT KEZELÉSE ÉS VÉDELME 38
19. A TÁRSASÁGI IRATOK SZEMÉLYES ADATAINAK KEZELÉSE ÉS VÉDELME 38
20. ÜZLETI TITOK KÖRÉBE TARTOZÓ ADATOK KEZELÉSE ÉS VÉDELME 38
21. „SZIGORÚAN BIZALMAS!" ADATOKAT TARTALMAZÓ DOKUMENTUMOK MINŐSÍTÉSE 39
22. A „SZIGORÚAN BIZALMAS!" JELZÉSSEL MINŐSÍTETT DOKUMENTUMOK KÉSZÍTÉSE, KEZELÉSE ÉS VÉDELME 39
23. VONATKOZÓ JOGSZABÁLYOK 40

MELLÉKLETEK **41**
1. számú melléklet - A közérdekű adatok megismerésére irányuló igényre és annak teljesítésére vonatkozó eljárásrend 42
2. számú melléklet – Új adatkezelés bejelentésének tartalma 46
3. számú melléklet - Minősítési javaslat 47
4. számú melléklet - Az ÁKK Zrt. adatvédelmi incidensekkel kapcsolatos eljárásrendje 48
5. számú melléklet – Vonatkozó jogszabályok 56

1. Általános rendelkezések

1.1. A Szabályzat célja és tárgya

Az Államadósság Kezelő Központ Zártkörűen Működő Részvénytársaság (továbbiakban: **ÁKK Zrt.**), mint adatkezelő célja, hogy a tevékenységével összefüggésben felmerülő személyes adatok kezelésével járó folyamatai, eljárásai során biztosítsa a személyes adatok védelmének megfelelő szintjét 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 szóló Európai Parlament és a Tanács (EU) 2016/679 rendelete (Általános Adatvédelmi Rendelet – továbbiakban: **GDPR**), valamint az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény és egyéb releváns jogszabályok szerint.

A szabályzat célja továbbá meghatározni mindazon belső rendelkezéseket, amelyek biztosítják az ÁKK Zrt. által vezetett nyilvántartások működésének törvényes megfelelőségét, valamint az adatvédelem alkotmányos elveinek, és az egyéb adatbiztonsági jogszabályi követelményeknek az érvényesülését, és megakadályozzák a jogosulatlan hozzáférést, az adatok megváltoztatását és jogosulatlan nyilvánosságra hozatalát.

Jelen szabályzat célja, hogy ismertesse az ÁKK Zrt. munkavállalóival a rájuk vonatkozó, illetve a tevékenységük végzése közben felmerülő személyes adatok kezelése során érvényesítendő szabályokat és eljárásokat.[1]

Az adatkezelési műveleteket az ÁKK Zrt. úgy tervezi meg és hajtja végre, hogy az érintettek magánszférájának védelme megfelelő módon biztosított legyen. A technika mindenkori fejlettségére tekintettel - megteszi azokat a technikai és szervezési intézkedéseket és kialakítja azokat az eljárási szabályokat, amelyek az adatbiztonság érvényre juttatásához szükségesek. Az adatokat védi különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, az adatok károsodása és véletlen elvesztése, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen.

Az ÁKK Zrt. adatfeldolgozó igénybevétele esetén gondoskodik arról, hogy a kiválasztott adatfeldolgozó a személyes adatok védelme érdekében megtegye a szükséges intézkedéseket, valamint kövesse az ÁKK Zrt. szabályzatait és egyedi utasításait. Az adatfeldolgozó kiválasztása

[1] Az ÁKK Zrt. munkavállalóinak személyes adatai kezelésére vonatkozó részletes Adatkezelési Tájékoztatóját a Munkaügyi Szabályzat 10. számú melléklete tartalmazza.

során az ÁKK Zrt. törekszik arra, hogy csakis olyan adatfeldolgozó kerüljön igénybevételre, amely megfelelő garanciákat nyújt arra vonatkozóan, hogy az adatvédelmi követelmények teljesülését biztosító technikai és szervezési intézkedéseket végrehajtja.

1.2. Az Adatkezelő személye és tevékenysége

Az ÁKK Zrt., mint köztulajdonban álló gazdasági társaság jogállását és tevékenységét kiemelkedően a Magyarország gazdasági stabilitásáról szóló 2011. évi CXCIV. törvény (Stabilitási tv.), az államháztartásról szóló 2011. évi CXCV. törvény (Áht.), az adott évre vonatkozó költségvetési törvények és a tőkepiacról szóló 2001. évi CXX. törvény (Tőkepiaci törvény) szabályozza.

Az ÁKK Zrt. tevékenységét különböző jogi és természetes személyekkel kötött szerződéses jogviszony keretein belül végzi.

1.3. A Szabályzat tárgyi hatálya

A Szabályzat hatálya az ÁKK Zrt.-nél folytatott valamennyi személyes adatot tartalmazó adatkezelésre kiterjed.

1.4. A Szabályzat alanyi hatálya

Jelen Szabályzat hatálya kiterjed az ÁKK Zrt. valamennyi munkavállalójára és a munkavégzésre irányuló egyéb jogviszonyban álló harmadik személyekre.

1.5. Fogalom meghatározások

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.

2. Különleges 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 adatok.

3. Adatkezelő: Az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely önállóan vagy másokkal együtt az adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja. A jelen Szabályzat hatálya alá tartozó adatkezelések tekintetében adatkezelő az ÁKK Zrt.

4. 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.

5. Adattovábbítás: Az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele.

6. Harmadik személy: 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.

7. Adatfeldolgozó: Az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy valamely az adatkezelővel kötött szerződése alapján – beleértve a jogszabály rendelkezése alapján történő szerződéskötést is – adatok feldolgozását végzi.

8. Adatfeldolgozás: Az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől, feltéve, hogy a technikai feladatot az adaton végzik.

9. Címzett: Az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, akivel vagy amellyel a személyes adatot közlik, függetlenül attól, hogy harmadik fél-e. Azon közhatalmi szervek, amelyek egy egyedi vizsgálat keretében az uniós vagy a tagállami joggal összhangban férhetnek hozzá személyes adatokhoz, nem minősülnek címzettnek; az említett adatok e közhatalmi szervek általi kezelése meg kell, hogy feleljen az adatkezelés céljainak megfelelően az alkalmazandó adatvédelmi szabályoknak.

10. Hozzájárulás: Az érintett akaratának önkéntes és meghatározott kinyilvánítása, amely megfelelő tájékoztatáson alapul, és amellyel félreérthetetlen beleegyezését adja a rá vonatkozó személyes adatok – teljes körű vagy egyes műveletekre kiterjedő kezeléséhez.

11. Tiltakozás: Az érintett nyilatkozata, amellyel személyes adatainak kezelését kifogásolja, és az adatkezelés megszüntetését, illetve a kezelt adatok törlését kéri.

12. Adattörlés: Az adat felismerhetetlenné tétele oly módon, hogy a helyreállítása többé nem lehetséges.

13. 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.

14. Technikai és szervezési intézkedések: Az adatkezelő által az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelően meghatározott eljárásrend annak biztosítása és bizonyítása céljából, hogy a személyes adatok kezelése a GDPR-ral összhangban történik. Ezeket az intézkedéseket az adatkezelő felülvizsgálja és szükség esetén naprakésszé teszi.

15. Adótitok[2]: az adózást érintő tény, adat, körülmény, határozat, végzés, igazolás vagy más irat. Az adótitokra vonatkozó rendelkezéseket, és a közösségi vámjog végrehajtásáról szóló törvény 16. § (9) bekezdésében foglalt rendelkezést kell alkalmazni a VPID szám megállapításával, nyilvántartásba vételével és nyilvántartásával összefüggő eljárásokra.

16. Banktitok[3]: minden olyan, az egyes ügyfelekről a pénzügyi intézmény rendelkezésére álló tény, információ, megoldás vagy adat, amely ügyfél személyére, adataira, vagyoni helyzetére, üzleti tevékenységére, gazdálkodására, tulajdonosi, üzleti kapcsolataira, valamint a pénzügyi intézmény által vezetett számlájának egyenlegére, forgalmára, továbbá a pénzügyi intézménnyel kötött szerződéseire vonatkozik. A hitelintézetekről és pénzügyi vállalkozásokról szóló törvény banktitokra vonatkozó rendelkezései szempontjából a pénzügyi intézmény ügyfelének kell tekinteni mindenkit, aki (amely) a pénzügyi intézménytől pénzügyi szolgáltatást vesz igénybe.

[2] Hatályos - 2003. évi XCII. törvény 53.§
[3] Hatályos - 2013. évi CCXXXVII. törvény 160.§

17. Bizalmas minősítés[4]: Amennyiben az adat nyilvánosságra hozatala, jogosulatlan megszerzése, módosítása vagy felhasználása, illetéktelen személy részére hozzáférhetővé, valamint az arra jogosult részére hozzáférhetetlenné tétele károsítja a minősítéssel védhető közérdeket.

18. Értékpapírtitok[5]**:** minden olyan, az ügyfélről a befektetési vállalkozás, a multilaterális kereskedési rendszer működtetője és az árutőzsdei szolgáltató rendelkezésére álló adat, amely az ügyfél személyére, adataira, vagyoni helyzetére, üzleti befektetési tevékenységére, gazdálkodására, tulajdonosi, üzleti kapcsolataira, illetve a befektetési vállalkozással és árutőzsdei szolgáltatóval kötött szerződéseire, számlájának egyenlegére és forgalmára vonatkozik.

19. Korlátozott terjesztésű minősítés[6]**:** Amennyiben az adat nyilvánosságra hozatala, jogosulatlan megszerzése, módosítása vagy felhasználása, illetéktelen személy részére hozzáférhetővé, valamint az arra jogosult részére hozzáférhetetlenné tétele hátrányosan érinti a minősítéssel védhető közérdeket.

20. Nemzeti minősített adat: a minősítéssel védhető közérdekek körébe tartozó, a minősítési jelölést az e törvényben, valamint az e törvény felhatalmazása alapján kiadott jogszabályokban meghatározott formai követelményeknek megfelelően tartalmazó olyan adat, amelyről - a megjelenési formájától függetlenül - a minősítő a minősítési eljárás során megállapította, hogy az érvényességi időn belüli nyilvánosságra hozatala, jogosulatlan megszerzése, módosítása vagy felhasználása, illetéktelen személy részére hozzáférhetővé, valamint az arra jogosult részére hozzáférhetetlenné tétele a minősítéssel védhető közérdekek közül bármelyiket közvetlenül sérti vagy veszélyezteti (a továbbiakban együtt: károsítja), és tartalmára tekintettel annak nyilvánosságát és megismerhetőségét a minősítés keretében korlátozza.

21. Közérdekű adat: Az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő és tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől, így különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre, annak

[4] Hatályos- 2009. évi CLV törvény 5.§ (4) bekezdés c) alpont
[5] Hatályos - 2007. évi CXXXVIII. törvény 4. § (2) bekezdés 27. alpont
[6] Hatályos- 2009. évi CLV törvény 5.§ (4) bekezdés d) alpont

eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat.

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

23. Szigorúan titkos minősítés: Amennyiben az adat nyilvánosságra hozatala, jogosulatlan megszerzése, módosítása vagy felhasználása, illetéktelen személy részére hozzáférhetővé, valamint az arra jogosult részére hozzáférhetetlenné tétele rendkívül súlyosan károsítja a minősítéssel védhető közérdeket.

24. Titkos minősítés[7]: Amennyiben az adat nyilvánosságra hozatala, jogosulatlan megszerzése, módosítása vagy felhasználása, illetéktelen személy részére hozzáférhetővé, valamint az arra jogosult részére hozzáférhetetlenné tétele súlyosan károsítja a minősítéssel védhető közérdeket.

25. Ügyfél:[8] A befektetési vállalkozásokról és az árutőzsdei szolgáltatókról, valamint az általuk végezhető tevékenységek szabályairól szóló 2007. évi CXXXVIII. törvény (a továbbiakban Bszt.) értelmében ügyfélnek minősül az, aki a Bszt. hatálya alá tartozó szolgáltatást veszi igénybe. A Bszt. értelmében szakmai ügyfélnek minősül az, aki megfelel a Bszt. 49. §-ban foglalt feltételeknek, illetve a 48. § szerint ilyennek minősül.

26. Üzleti titok[9]: Üzleti titok a gazdasági tevékenységhez kapcsolódó, titkos - egészben, vagy elemeinek összességeként nem közismert vagy az érintett gazdasági tevékenységet végző személyek számára nem könnyen hozzáférhető -, ennélfogva vagyoni értékkel bíró olyan tény, tájékoztatás, egyéb adat és az azokból készült összeállítás, amelynek a titokban tartása érdekében a titok jogosultja az adott helyzetben általában elvárható magatartást tanúsítja.

27. Felügyeleti hatóság: Egy tagállam által a GDPR 51. cikkének megfelelően létrehozott független közhatalmi szerv; Magyarországon a Nemzeti Adatvédelmi és Információszabadság Hatóság.

2. Adatvédelmi alapelvek

2.1. Jogszerűség, tisztességes eljárás, átláthatóság

[7] Hatályos- 2009. évi CLV törvény 5.§ (4) bekezdés b) alpont
[8] Hatályos - 2001. évi CXX. törvény 369.§ (2) bekezdés
[9] Hatályos - 2018. évi LIV. törvény 1.§ (1) bekezdés

A személyes adatok kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni. A természetes személyek számára átláthatónak kell lennie, hogy a rájuk vonatkozó személyes adataikat hogyan gyűjtik, használják fel, azokba, hogy tekintenek bele vagy milyen egyéb módon kezelik, valamint azzal összefüggésben, hogy a személyes adatokat milyen mértékben kezelik vagy fogják kezelni. A személyes adatoknak a kezelésük céljára alkalmasoknak és relevánsaknak kell lenniük. A személyes adatokat olyan módon kell kezelni, amely biztosítja azok megfelelő szintű biztonságát és bizalmas kezelését, többek között annak érdekében, hogy megakadályozza a személyes adatokhoz és a személyes adatok kezeléséhez használt eszközökhöz való jogosulatlan hozzáférést, illetve azok jogosulatlan felhasználását.

2.2. Célhoz kötöttség

A személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történhet, azok kezelése nem történhet a célokkal össze nem egyeztethető módon. Nem minősül az eredeti céllal össze nem egyeztethetőnek a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból történő további adatkezelés.

Az ÁKK Zrt. törli a személyes adatot minden olyan esetben, amikor az adatkezelés célja megszűnt és törvényi kötelezettség, vagy jogos érdek nem áll fenn az adat további tárolásával, kezelésével kapcsolatban.

2.3. Adattakarékosság

A személyes adatok az adatkezelés céljai szempontjából megfelelőek és relevánsak kell, hogy legyenek, és a szükségesre kell korlátozódniuk. Személyes adatok csak abban az esetben kezelhetők, ha az adatkezelés célját egyéb eszközzel ésszerű módon nem lehetséges elérni. Annak biztosítása érdekében, hogy a személyes adatok tárolása a szükséges időtartamra korlátozódjon, az ÁKK Zrt. törlési vagy rendszeres felülvizsgálati határidőket állapít meg. Biztosítani kell, hogy a személyes adatok tárolása a lehető legrövidebb időtartamra korlátozódjon. A kezelt adatok körét a célhoz szükséges minimumra kell korlátozni.

2.4. Pontosság

A személyes adatoknak pontosnak, teljesnek, aktuálisnak és szükség esetén naprakésznek kell lenniük; minden ésszerű intézkedést meg kell tenni annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatok haladéktalanul törölve vagy helyesbítve legyenek.

2.5. Korlátozott tárolhatóság

A személyes adatok tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig tegye lehetővé. A személyes adatok ennél hosszabb ideig történő tárolására csak akkor kerülhet sor, amennyiben a személyes adatok kezelésére közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból kerül majd sor, a GDPR-ban az érintettek jogainak és szabadságainak védelme érdekében előírt megfelelő technikai és szervezési intézkedések végrehajtására is figyelemmel.

2.6. Integritás és bizalmas jelleg

Az ÁKK Zrt. a személyes adatokat védi 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 ellen.

2.7. Elszámoltathatóság

Az adatkezelés tényének, helyének és céljának, az adatkezelő személyének, valamint az adatkezelési politikának nyilvánosnak kell lennie. Az ÁKK Zrt. a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint az érintettek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével, mind az adatkezelés módjának meghatározásakor, mind pedig az adatkezelés során olyan megfelelő technikai és szervezési intézkedéseket hajt végre, amelyek célja egyrészt az adatvédelmi elvek, másrészt a GDPR-ban foglalt követelmények teljesítése és az érintettek jogainak védelméhez szükséges garanciák beépítése az adatkezelési folyamatába.

3. Az adatkezelés jogalapjai

3.1. Az érintett önkéntes hozzájárulása

A GDPR 6. cikk (1) bekezdésének a) pontja szerint az érintett önkéntes hozzájárulása alapján kerülhet sor az adatkezelésre. Amennyiben egyéb jogalap alapján az ÁKK Zrt. nem jogosult az Érintett adatainak kezelésére, az Érintett jogosult az adatkezelőhöz intézett írásos bejelentés

útján az adatkezeléshez adott hozzájárulását részlegesen vagy teljesen visszavonni, illetve az adatai törlését kérni. Papír alapú hozzájárulás esetén az ÁKK Zrt. a hozzájáruló nyilatkozat megőrzésére köteles.

Az ÁKK Zrt. mint adatkezelő előre megfogalmazott hozzájárulási nyilatkozatról köteles gondoskodni, amelyet érthető és könnyen hozzáférhető formában köteles rendelkezésre bocsátani, nyelvezetének pedig világosnak és egyszerűnek kell lennie, és nem tartalmazhat tisztességtelen feltételeket.

Ha az adatkezelés egyszerre több célt is szolgál és mindegyik jogalapja az érintett hozzájárulása, akkor a hozzájárulást az összes adatkezelési célra vonatkozóan meg kell kérni.

A 16. életévét be nem töltött gyermek esetén a gyermek feletti szülői felügyeletet gyakorló személy adja meg a hozzájárulást, illetve engedélyezi az adatkezelést.

3.2. Szerződés teljesítéséhez szükséges adatok

A GDPR 6. cikk (1) bekezdésének b) pontja alapján 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. A szerződés megkötéséhez és teljesítéséhez szükséges adatokon felül, kizárólag ezen jogalap alapján további adatok nem kezelhetőek.

3.3. Adatkezelő jogi kötelezettségének teljesítéséhez szükséges adatkezelés

A GDPR 6. cikk (1) bekezdésének c) pontja alapján az adatkezelés olyan jogi kötelezettség teljesítéséhez szükséges, amely az ÁKK Zrt.-re vonatkozik. Az ÁKK Zrt. jogosult a rá kötelező erővel rendelkező jogszabályokban előírt, kifejezett adatkezelésre (pl.: nyomdai úton előállított állampapír kellékének számító személyes adatok, számviteli előírások).

3.4. Létfontosságú érdek védelme érdekében történő adatkezelés

A GDPR 6. cikk (1) bekezdésének d) pontja alapján az adatkezelés az Érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges.

3.5. Közérdekű feladat végrehajtásához szükséges adatkezelés

A GDPR 6. cikk (1) bekezdésének e) pontja alapján az adatkezelés közérdekű vagy az Adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges.

3.6. Jogos érdek érvényesítése érdekében történő adatkezelés

A GDPR 6. cikk (1) bekezdésének f) pontja alapján az adatkezelés az ÁKK Zrt. vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges.

4. Az adatkezeléssel kapcsolatos rendelkezések

4.1. Adatállományok kezelése

Az ÁKK Zrt. biztosítja, hogy a személyes adatok nyilvántartásának módja és adattartalma a mindenkor hatályos jogszabályoknak megfeleljen. A jogszabályon alapuló adatkezelések kötelezőek, azokról az érintettek tájékoztatást kérhetnek. Az ÁKK Zrt. gondoskodik az eltérő célú adatkezelések megfelelő, logikai elkülönítéséről.

Az ÁKK Zrt. az elektronikus és a papíralapú nyilvántartásokat egységes elvek alapján, a nyilvántartások adathordozóinak különbözőségéből adódó jellemzők figyelembe vételével kezeli.

A jelen Szabályzat szerinti elvek és kötelezettségek az elektronikus és a papíralapú nyilvántartások esetében egyaránt érvényesülnek.

Az ÁKK Zrt. az adatkezelési nyilvántartás rendszerének felépítése, a jogosultságok meghatározása, és egyéb szervezeti intézkedések útján gondoskodik arról, hogy a nyilvántartásokban szereplő adatokat csak azok a munkavállalók, és egyéb az ÁKK Zrt. érdekkörében eljáró személyek ismerhessék meg, akiknek erre munkakörük, feladatuk ellátása érdekében szükségük van.

Az ÁKK Zrt. a nyilvántartások papíralapú dokumentumait az adatbiztonság követelményeire tekintettel tárolja, és gondoskodik azok biztonságos őrzéséről.

Az adatbiztonsági előírások biztosítják, hogy az adatokhoz csak célhoz kötötten, ellenőrzött körülmények között és csak azon személyek férjenek hozzá, akiknek a feladataik ellátása érdekében erre szükségük van.

Az ÁKK Zrt. lehetőség szerint törekszik az adatminimum elvének érvényesülésére, annak érdekében, hogy az egyes munkavállalók, és egyéb, az ÁKK Zrt. érdekkörében eljáró személyek csak a szükséges személyes adatokhoz férjenek hozzá.

Az adatállományok kezelésére, azok biztonságos őrzésére, a hozzáférési jogokra, adatok, dokumentációk felhasználására az ÁKK Zrt. szervezetén belül hatályos szabályzatok, utasítások az irányadók. Ezen szabályzatok, utasítások a jelen Szabályzat és az irányadó jogszabályok – elsősorban a GDPR – elveinek és rendelkezéseinek érvényre juttatását szolgálják.

4.2. A levéltári anyag kezelése

Az ÁKK Zrt., mint közfeladatot ellátó gazdasági társaság a levéltári anyag védelmére vonatkozó szabályozás hatálya alá tartozik. A köziratokról, közlevéltárakról, és a magánlevéltári anyag védelméről szóló 1995. évi LXVI. törvény alapján az ÁKK Zrt.-nél keletkezett iratok köziratok, melyek megőrzésére a hivatkozott törvény, a törvény alapján kiadott iratkezelési szabályok, valamint irattári terv vonatkozik.

Az ÁKK Zrt. a levéltári anyagot a vonatkozó szabályok alapján akkor is nyilvántartja, ha egyébként a dokumentumokban lévő személyes adatok kezelésének célja megszűnt. Ebben az esetben az adatkezelés jogalapja a levéltári anyagra vonatkozó törvényi szabályozás. Az ÁKK Zrt. a levéltári anyag őrzésére vonatkozó szabályozásról az érintetteknek kérésre tájékoztatást ad.

4.3. Az adatkezelés típusai

Az ÁKK Zrt. ügyviteli, illetve nyilvántartási típusú adatkezelést végez.

Az ügyviteli típusú adatkezelés szorosan az ügy feldolgozásához kapcsolódik, alapvető rendeltetése az adott ügy lefolytatásához, az eljárás szereplőinek azonosításához és az ügy befejezéséhez szükséges adatok biztosítása. Az ügyviteli típusú adatkezelés során a személyes adatok kizárólag az adott ügy irataiban és az ügyviteli segédletekben szerepelnek, kezelésükre csak az alapul szolgáló irat selejtezéséig van lehetőség.

A nyilvántartási típusú adatkezelés az előre meghatározott szempontok alapján gyűjtött személyes adatfajtákból strukturált adatállományt hoz létre, az adatkezelés időtartama alatt biztosítva az adatok különböző jellemzők alapján történő visszakereshetőségét, automatizált nyilvántartások esetében a lekérdezhetőségét (pl. szerződéstár). Az egyes ügyekkel összefüggésben gyűjtött adatok kezelése ebben az esetben elválik az alapeljárástól, az adatok kezelésének időtartamát az adatok kezelésére felhatalmazást adó törvény, vagy az Érintett beleegyezésében foglaltak határozzák meg.

4.4. Az adatvédelem ÁKK Zrt.-n belüli szervezete

Az adatvédelmi előírások alkalmazása során az adatkezelő vezetője az ÁKK Zrt. vezérigazgatója.

4.4.1. A vezérigazgató

- felelős az ÁKK Zrt. adatkezelésének jogszerűségéért;
- gondoskodik az adatkezelés személyi és tárgyi feltételeinek biztosításáról, ennek keretében
  - az adatvédelemre és adatkezelésre vonatkozó belső szabályzat kiadásáról,
  - belső adatvédelmi felelőst, illetve adatvédelmi tisztviselőt jelöl ki;
- az ÁKK Zrt., mint adatkezelő tekintetében meghozza az adatkezelésre vonatkozó döntéseket;
- kivizsgáltatja az ellenőrzések során feltárt hiányosságokat, gondoskodik a jogszabálysértő körülmények megszüntetéséről.

4.4.2. A szervezeti egységek vezetői

Felelősek az irányításuk alá tartozó szervezeti egységek adatkezelésének jogszerűségéért, a Szabályzatban foglaltak végrehajtásáért.

Jogosulatlan hozzáférés vagy az adatvédelmi előírások egyéb megsértésének észlelése esetén intézkedést tesznek annak megszüntetésére, indokolt esetben kezdeményezik a felelősségre vonási eljárás lefolytatását.

4.4.3. Belső adatvédelmi felelős/adatvédelmi tisztviselő

- közreműködik, illetve segítséget nyújt az adatkezeléssel összefüggő döntések meghozatalában, valamint az érintettek jogainak biztosításában,
- ellenőrzi az adatkezelésre vonatkozó jogszabályok, valamint a Szabályzat rendelkezéseinek és az adatbiztonsági követelményeknek a megtartását,
- kivizsgálja a hozzá érkező bejelentéseket; jogosulatlan adatkezelés észlelése esetén annak megszüntetésére hívja fel az ÁKK Zrt. vezérigazgatóját, illetve javaslatot tesz a jogszerű adatkezelést megsértő munkavállaló személyi felelősségre vonására,
- elkészíti és módosítja a Szabályzatot,
- vezeti a belső adatvédelmi, adattovábbítási és incidens nyilvántartást,
- gondoskodik az adatvédelmi ismeretek oktatásáról,
- együttműködik az ÁKK Zrt. adatvédelmi és adatbiztonsági intézményrendszerének kiépítésében, működtetésében, valamint ennek keretében a személyes adatok védelméhez szükséges személyi, tárgyi és technikai feltételek biztosítását célzó intézkedések megtételében.

4.4.4. A munkavállalók; harmadik személyek

- függetlenül a foglalkoztatás jellegétől (alkalmazott, megbízott vagy egyéb külső személy) felelősek az általuk kezelt, feldolgozott adatok minősítése szerinti titoktartásért (lásd: SZMSZ, Ügyviteli és egyéb vonatkozó szabályzat) és e Szabályzat betartásáért,
- felelősek az általuk végzett adatkezelés jogszerűségéért;
- az adatkezelést érintő érdemi döntést nem hozhatnak, a tudomásukra jutott személyes adatokat kizárólag az adatkezelő rendelkezései szerint dolgozhatják fel, saját célra adatkezelést nem végezhetnek, továbbá a személyes és egyéb bizalmas adatokat az ÁKK Zrt. rendelkezései szerint kötelesek tárolni és megőrizni;
- kötelesek e Szabályzat 2. számú mellékletét képező adatlapon írásban a belső adatvédelmi felelős felé jelenteni az új adatkezelési tevékenységet.
- kötelesek e Szabályzat 4. számú mellékletét képező eljárásrend szerint, írásban, késedelem nélkül jelenteni, ha adatvédelmet vagy adatbiztonságot veszélyeztető eseményt, adatvédelmi rendelkezések sérelmét, annak következményeit észlelik, bekövetkezését valószínűsítik (lásd: Adatvédelmi incidens), vagy ha a Szabályzat rendelkezéseinek érvényesülése bármilyen módon ellehetetlenül.

4.5. Adatbiztonság

Az ÁKK Zrt. gondoskodik a személyes adatok biztonságáról, megteszi azokat a technikai és szervezési intézkedéseket és kialakítja azokat az eljárási szabályokat, amelyek az irányadó jogszabályok, adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.

Az ÁKK Zrt. a személyes adatokat megfelelő intézkedésekkel védi a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen.

Az adatbiztonság szabályainak érvényesüléséről az ÁKK Zrt. külön szabályzatok, utasítások, eljárási rendek útján gondoskodik. Az ÁKK Zrt. az adatbiztonság feltételeinek érvényesítése érdekében gondoskodik az érintett munkatársak megfelelő felkészítéséről.

Az ÁKK Zrt. az adatok biztonságát szolgáló intézkedések meghatározásakor és alkalmazásakor tekintettel van a technika mindenkori fejlettségére.

a) Informatikai nyilvántartások védelme

Az ÁKK Zrt. az informatikai védelemmel kapcsolatos feladatai körében gondoskodik különösen:

- a jogosulatlan hozzáférés elleni védelmet biztosító intézkedésekről, ezen belül a szoftver és hardver eszközök védelméről, illetve a fizikai védelemről (hozzáférés védelem, hálózati védelem);
- az adatállományok helyreállításának lehetőségét biztosító intézkedésekről, ezen belül a rendszeres biztonsági mentésről és a másolatok elkülönített, biztonságos kezeléséről;
- az adatállományok vírusok elleni védelméről (vírusvédelem);
- az adatállományok, illetve az azokat hordozó eszközök fizikai védelméről, ezen belül a tűzkár, vízkár, villámcsapás, egyéb elemi kár elleni védelemről, illetve az ilyen események következtében bekövetkező károsodások helyreállíthatóságáról (archiválás, tűzvédelem, katasztrófa központ üzemeltetése).

b) Papíralapú nyilvántartások védelme

Az ÁKK Zrt. a papíralapú nyilvántartások védelme érdekében megteszi a szükséges intézkedéseket különösen a fizikai biztonság, illetve tűzvédelem tekintetében.

A munkavállalók, és egyéb, az ÁKK Zrt. érdekében eljáró személyek az általuk használt, vagy birtokukban lévő, személyes adatokat is tartalmazó adathordozókat, függetlenül az adatok rögzítésének módjától, kötelesek biztonságosan őrizni, és védeni a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés ellen.

c) Az adatbiztonság szabályozása

Az adatkezelés biztonsága megvalósítása érdekében az ÁKK Zrt. fizikai, logikai és adminisztratív kontrollokat alkalmaz együttesen.

Az ÁKK Zrt. legalább az alábbi fizikai kontrollokat alkalmazza:

- az ÁKK Zrt. a jogosulatlan személyek belépésének kiszűrését portaszolgálat igénybevételével biztosítja, hogy épületébe/irodáiba jogosulatlan személyek ne léphessenek be (egyszerű kulcsos beléptetés, ahol a kulcs csak belépésre jogosultaknak áll rendelkezésre)
- az ÁKK Zrt. az általa mind elektronikusan, mind pedig papír alapon kezelt adatokhoz való jogosulatlan hozzáférés elkerülése érdekében biztosítja, hogy a kezelt adatokhoz fizikailag ne férhessen hozzá arra jogosulatlan személy (az irodák, szerverszoba zárása; szükséges helyeken monitor fóliák alkalmazása; monitorok olyan módon történő elhelyezése, hogy az azon szereplő adatokra kizárólag a jogosultak láthassanak rá;

- csak az ÁKK Zrt. által jóváhagyott, az Informatikai Főosztály által engedélyezett, *McAfee ePO server által menedzselt McAfee File and Removable Media Protection* (fájlok, könyvtárak titkosítása helyi és külső adathordozó eszközökön) által felügyelt, titkosított és jelszóval védett - adathordozót lehessen a számítógépekhez csatlakoztatni).

Az ÁKK Zrt. legalább az alábbi logikai kontrollokat alkalmazza:
Az ÁKK Zrt. biztosítja, hogy az általa kezelt adatokhoz kizárólag az arra megfelelő jogosultsággal rendelkezők férjenek hozzá (a jogosultsági szintek meghatározása munkakörönként; számítógépes adatbázisokhoz való hozzáférés jogosultsági szinteknek megfelelő beállítása; a belső számítógépes hálózatba való belépés felhasználó névhez és jelszóhoz kötése).

Az ÁKK Zrt. legalább az alábbi adminisztratív kontrollokat alkalmazza:

- az ÁKK Zrt. biztosítja, hogy a személyes adatokhoz való esetleges hozzáférés dokumentációkban nyomon követhető legyen (tevékenység-naplózás; épületbe való beengedés naplózása).
- az ÁKK Zrt. biztosítja olyan iratkezelési eljárásrend kialakítását, hogy a hozzá tévesen beérkező személyes adatokat tartalmazó iratok a lehető leghamarabb kiszűrésre kerüljenek és azokat a lehető legszűkebb személyi kör ismerje meg.

Az ÁKK Zrt. által működtetett informatikai rendszerek felhasználói, a munkavállalók és a személyes adatokkal egyéb módon kapcsolatba kerülő személyek a személyes adatok védelme érdekében kötelesek megtartani az alábbi előírásokat:

- A munkavégzés során keletkezett személyes adatot is tartalmazó elektronikus dokumentumokat csak a munkavégzés céljára szolgáló számítástechnikai eszközökön nyithatják meg a munkát végzők. A munkavégzés céljára szolgáló eszközök és szoftverek hozzáférési kódjait a munkavállalók bizalmasan kötelesek kezelni, azokat még közvetlen kollégáikkal sem oszthatják meg. Az ilyen, személyes adatokat is tartalmazó elektronikus dokumentumok csak és kizárólag az arra kijelölt hálózati meghajtón (könyvtárba rendezetten) tárolhatók.

- A munkavégzés céljára átadott notebook-ok, tabletek és telefonok esetében a munkavállalók kötelesek az általuk használt profilt jelszóval védeni és azt a hozzátartozóik, vagy más személyek számára megadni tilos. A munkavégzésre használt notebook-ot, amelyen az ÁKK Zrt. által kezelt, vagy feldolgozott személyes adat is

megtalálható, minden esetben jelszavas védelemmel kell használni. Munkavállaló köteles az ÁKK Zrt. által biztosított készüléken megfelelő bonyolultságú jelszót létrehozni, továbbá a készüléket a munkaviszonyának fennállása alatt folyamatosan jelszavas védelemmel ellátva használni, melyet kizárólag a munkavállaló ismer.

Munkavállaló köteles az általa használt jelszót az eszköz visszaadásának napján törölni vagy az ÁKK Zrt. által megadott alap jelszóra átállítani és az eszközt így visszaszolgáltatni, ennek megtörténtét az átvételt végző Informatikai Főosztály ellenőrzi.

A papír alapú személyes adatokat tartalmazó munkadokumentumokat olyan módon kell kezelni, tárolni, hogy azokat csak az erre a feladatra megbízott munkavállaló érhesse el, aki köteles azokat mások által elhatárolt, zárt helyen tartani, ha azok használata már nem szükséges, olyan módon kell megsemmisíteni (pl: irat „konfettis" ledarálásával), hogy a megsemmisítést követően ne lehessen azok tartalmát megállapítani.
A munkavállaló munkaviszonya, megbízása, egyéb feladatellátásra szolgáló jogviszonya megszűnése esetén minden személyes adatot is tartalmazó papír alapú és elektronikus iratot, adatot köteles a foglalkoztatásának utolsó napját megelőzően az ÁKK Zrt. részére visszaszolgáltatni, azokról másolatot nem tarthat magánál, melyről *2 példányban* átadás-átvételi jegyzőkönyvet kell készíteni, melyből az egyik példány a munkavállalót illeti.

Tilos magánhasználatú eszközön az ÁKK Zrt. kezelésében lévő személyes adatot tárolni, kivéve, ha a tárolás a munkavégzéshez elengedhetetlenül szükséges és a tárolást a munkavégzést követően megszüntetik.

Minden munkavállaló köteles az általa használt munkaterületet olyan módon használni, hogy azon az ÁKK Zrt. kezelésében lévő, személyes adatot is tartalmazó dokumentumok lehetőség szerint szabadon ne legyenek hozzáférhetők (Tiszta Asztal Politika). Ilyen intézkedésnek minősül különösen: számítástechnikai eszközök jelszavas védelme, az irodahelyiség zárása, az iratok elhelyezése védett, zárható helyen történő tárolása (a mindenkor hatályos az ÁKK Zrt. fizikai biztonsági és beléptetési rendjéről valamint a rendezett munkakörnyezettel kapcsolatos elvárásról szóló szabályzat előírásainak megfelelően).
Minden munkavállaló köteles biztosítani és megfelelő intézkedéseket megtenni annak érdekében, hogy az ÁKK Zrt. irodaépületébe a nem az ÁKK Zrt.-vel munkaviszonyban, vagy

egyéb munkavégzésre irányuló egyéb jogviszonyban álló személy csak az ÁKK Zrt. munkavállalójának, vagy megbízottjának kíséretében léphessen be.

Az ÁKK Zrt. területére belépni jogosult személyek (pl. a saját, vagy a bérlemény ingatlanüzemeltetőjének (jelenleg: ATQ Zrt.) megbízásából karbantartási munkát végző személyek, egyéb informatikai környezeten karbantartást végző személyek, külső fejlesztők, szervízelők, takarítók, stb.) az ÁKK Zrt. által kezelt személyes adatok megismerésére nem jogosultak és kötelesek megtenni mindent annak érdekében, hogy az ÁKK Zrt. kezelésében álló személyes adatok biztonságban legyenek, az ennek megsértéséből az ÁKK Zrt.-t ért kárért az adatvédelmi incidenst előidéző személy teljes felelősséggel tartozik.

Személyes adatok csak biztonságos kommunikációs csatorna alkalmazásával, vagy megfelelő titkosítási megoldással adhatók át más személynek (pl. jelszóval védett adathordozó, vagy titkosított állomány). Ellenkező értesítésig az ÁKK Zrt. belső levelezési rendszerén belüli adatáramlás biztonságos kézbesítési csatornának tekintendő. Külső adatátadás során gondoskodni kell a személyes adatok titkosításáról (PDF dokumentumok jelszóval történő ellátása, NetLock által kiadott titkosítói tanúsítvány használata, SSL kapcsolat), vagy egyedi titkosítás használatával, a felhasználónév és jelszó elkülönített csatornán (pl.: SMS) keresztül történő küldésével, papír alapon pedig zárt borítékon keresztüli átadással.

Amennyiben az ÁKK Zrt. más adatkezelőtől, az adathoz kapcsolódó rendelkezéssel fogad személyes adatot, valamennyi, az adattal érintkező felhasználónak kötelessége az adattovábbító rendelkezéseit figyelembe venni.

Nem adható át külső személynek titoktartási nyilatkozat hiányában személyes adat, hasonlóan egyéb, az ÁKK Zrt. által bizalmasnak minősített adatokhoz.

4.6. Adatvédelmi hatásvizsgálat

A GDPR 35. cikke értelmében az adatkezelést megelőzően adatvédelmi hatásvizsgálat elvégzése kötelező, amennyiben az adatkezelés valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve.
Az ÁKK Zrt. a 29. cikk szerinti munkacsoport gyakorlatára hivatkozással általánosságban megállapítja, hogy az általa végzett adatkezelés valószínűsíthetően nem jár magas kockázattal a természetes személyek jogaira és szabadságaira nézve (GDPR 35. cikk (1) bekezdése), így az adatkezelést megelőzően nincs szükség adatvédelmi hatásvizsgálat elvégzésére.

Amennyiben az újonnan felmerülő adatkezelés tekintetében esetlegesen felmerül a hatásvizsgálat elvégzésének szükségessége, az ÁKK Zrt. vezérigazgatója dönt a hatásvizsgálat elvégzéséről.

5. Érintettek joggyakorlásának belső eljárásrendje

Az Érintettet (természetes személy) az alábbi jogosultságok illetik meg az ÁKK Zrt. adatkezelése esetén:

5.1. Tájékoztatás és a személyes adatokhoz való hozzáférés joga

a) Az érintett bármikor jogosult tájékoztatást kérni az ÁKK Zrt. által kezelt rá vonatkozó személyes adatokról. A tájékoztatás az adott adatkezelésről készült tájékoztatóban megjelölt elektronikus e-mail címen, postai levélben.
b) Az ÁKK Zrt. a kérelem kézhezvételétől számított ***30*** *(harminc)* ***napon belül*** adja meg a kért tájékoztatást.
c) A tájékoztatás keretében a belső adatvédelmi felelős – vagy a szerződésben erre a feladatra kijelölt adatfeldolgozó, közös adatkezelő – köteles az érintettre vonatkozó, ÁKK Zrt. által kezelt adatokról és a fentiekről tájékoztatást adni (az adott adatkezelésre alkalmazandó minta, vagy egyedileg – az adatfeldolgozást végző és a belső adatvédelmi felelős együttműködésében - kidolgozásra kerülő tájékoztató szerint.
d) A tájékoztatást az érintett által kért formában kell megadni, erre irányuló kifejezett kérés hiányában elsősorban email-en keresztül, másodsorban postai küldeményként kell megadni, amennyiben az ÁKK Zrt. számára rendelkezésre áll a kommunikációs forma használatához szükséges adat és amennyiben az érintett személyazonossága kétséget kizáróan megállapítható.
e) Ha az ÁKK Zrt. bizonyítani tudja, hogy nincs abban a helyzetben, hogy azonosítsa az érintettet, erről lehetőség szerint őt megfelelő módon tájékoztatja. Ilyen esetekben az érintett hozzáférési jogát, a helyesbítés és törlés kérésének jogát, az adatkezelés korlátozásához való jogát, az ezekhez kapcsolódó értesítési jogot, valamint adathordozhatósághoz való jogot az ÁKK Zrt. nem biztosítja, kivéve, ha az érintett abból a célból, hogy az említettek szerinti jogát gyakorolja, az azonosítását lehetővé tevő kiegészítő információkat nyújt.

f) A panaszok kezelésével kapcsolatban a személyes adatok kezelésében részt vevő munkavállalók, egyéb személyek tájékoztatást kötelesek adni az adatvédelemért felelős személy részére.
g) Az érintett által kért további másolatokért az ÁKK Zrt. az adminisztratív költségeken alapuló, ésszerű mértékű díjat számíthat fel.

5.2. Törléshez (elfeledtetéshez) való jog

Az érintett jogosult arra, hogy kérésére az ÁKK Zrt. indokolatlan késedelem nélkül törölje a rá vonatkozó személyes adatokat, az ÁKK Zrt. 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, amelyekből azokat gyűjtötték vagy más módon kezelték;
b) az érintett visszavonja az adatkezelés alapját szolgáló hozzájárulását és az adatkezelésnek más jogalapja nincs;
c) az érintett a közérdekű, valamint az ÁKK Zrt. vagy harmadik fél jogos érdekeinek érvényesítéséhez szükséges adatkezelés ellen tiltakozik és nincs elsőbbséget élvező jogszerű ok az adatkezelésre, vagy az érintett a közvetlen üzletszerzés céljából beszerzett adatainak kezelése ellen tiltakozik;
d) a személyes adatokat jogellenesen kezelte az ÁKK Zrt.;
e) a személyes adatokat az ÁKK Zrt.-re alkalmazandó uniós vagy tagállami jogban előírt jogi kötelezettség teljesítéséhez törölni kell;
f) a személyes adatok gyűjtésére a GDPR szerinti, információs társadalommal összefüggő szolgáltatások kínálásával kapcsolatosan került sor.

Amennyiben az ÁKK Zrt. nyilvánosságra hozta a személyes adatot, és azt törölni köteles, az elérhető technológia és a megvalósítás költségeinek figyelembevételével megteszi az ésszerűen elvárható lépéseket – ideértve technikai intézkedéseket – annak érdekében, hogy tájékoztassa az adatokat kezelő adatkezelőket, hogy az érintett kérelmezte tőlük a szóban forgó személyes adatok másolatának, illetve másodpéldányának törlését.

A törlést nem kell teljesíteni, amennyiben az adatkezelés:

a) véleménynyilvánítás szabadságához, vagy a tájékoztatáshoz való jog gyakorlása céljából szükséges,
b) jogi igények előterjesztéséhez, érvényesítéséhez és védelméhez szükséges,

c) jogi kötelezettség teljesítése miatt szükséges,
d) közérdekű archiválás, tudományos, vagy történelmi kutatás, statisztikai célból szükséges és az adattörlés lehetetlenné tenné, vagy komolyan veszélyeztetné az adatkezelés céljának teljesítését,
e) az informatikai rendszerek konzisztens, jogszerű működésének fenntartása érdekében szükséges.

Az ÁKK Zrt. továbbá törli vagy anonimizálja az érintettre vonatkozó, az informatikai rendszereiben, valamint papír alapú dokumentációiban szereplő személyes adatokat, ha jogszabály máshogy nem rendelkezik és a személyes adat kezeléséhez fűződő cél megszűnt.

Ha a személyes adat törlése nem valósítható meg az azt tartalmazó irat sérelme nélkül:

a) amennyiben az irat megőrzéséhez az ÁKK Zrt., vagy harmadik személy jogos érdeke fűződik, az iratot az ÁKK Zrt. az iratkezelési szabályok szerinti időtartamig megőrzi, törlési kérelem esetén az iratot zártan kezeli és erről az érintettet értesíti, és az iratot a személyes adattal együtt az iratkezelési szabályban meghatározott időtartam lejártát követően megsemmisíti;
b) amennyiben az irat megőrzéséhez az ÁKK Zrt.-nek és harmadik személynek sem fűződik jogos érdeke, az iratot a személyes adattal együtt megsemmisíti;
c) az adatok törlése iránt minden esetben az adatvédelemért felelős személy a személyes adat kezelésével kapcsolatban érintett szervezeti egységgel, informatikai rendszer üzemeltetéséért felelős vezetőjével együttműködésben intézkedik.

Az ÁKK Zrt. informatikai rendszereiből a személyes adatot – az adott informatikai rendszer adottságai szerint - visszaállíthatatlanul törli, vagy anonimizálja, továbbá az elérhető technológia és a megvalósítás költségeinek figyelembevételével megteszi az ésszerűen elvárható lépéseket és gondoskodik arról, hogy amennyiben az archivált változatot helyreállítani szükséges, a helyreállított változatban is kerüljön törlésre, illetve anonimizálásra az archiválás időpontja óta bekövetkezett személyes adat törlés, melyért az informatikai rendszerért felelős személy felel.

Amennyiben a helyreállíthatatlan törlés az adott informatikai rendszer sajátosságából következő okból nem kivitelezhető, ÁKK Zrt. az adat logikai törlését hajtja végre.

Az anonimizálás keretében a személyes adatot olyan azonosítóra kell lecserélni, amely megakadályozza, hogy a személyes adathoz tartozó további adatok a későbbiekben kapcsolatba hozhatók legyenek az érintettel.

A papír alapú, az érintett adatait tartalmazó dokumentációk esetében azok jegyzőkönyvvel rögzített megsemmisítéséről kell gondoskodni. A jegyzőkönyvben rögzíteni kell - a megsemmisített iratok típusát, a megsemmisített iratok beazonosíthatóságához szükséges információkat, a megsemmisítés időpontját és a megsemmisítést végző személy nevét, beosztását, külső partner esetén a külső partner nevét.

5.3. Az adatkezelés elleni tiltakozás kezelése

Az érintett a saját helyzetével kapcsolatos okokból bármikor tiltakozhat személyes adatainak kezelése ellen, ha az adatkezelés a GDPR 6. cikk (1) bekezdés e) vagy f) pontján alapul, illetve az érintett jogosult arra, hogy bármikor tiltakozzon a rá vonatkozó személyes adatok közvetlen üzletszerzés célból történő kezelése ellen, ideértve a profilalkotást is. Ha az érintett tiltakozik a személyes adatok közvetlen üzletszerzés érdekében történő kezelése ellen, akkor a személyes adatait a továbbiakban e célból nem kezeli az ÁKK Zrt.

Az ÁKK Zrt. a személyes adatokat nem kezelheti tovább, kivéve, ha 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. Az érintett tiltakozni írásban (e-mailben vagy postai úton) tud. Az adatvédelemért felelős személy a legrövidebb időn belül azonosítja az érintettet, a tiltakozást a kérelem benyújtásától számított legrövidebb időn belül megvizsgálja, annak megalapozottsága kérdésében döntést hoz, és döntéséről a kérelmezőt tájékoztatja.

5.4. A kezelt adatok helyesbítéséhez, kiegészítéséhez való jog

Az érintett bármikor jogosult a helytelenül rögzített adatainak helyesbítését kérni. Amennyiben az érintett jelzi, hogy az ÁKK Zrt. által kezelt bármely adata nem felel meg a valóságnak, az adatvédelemért felelős személy azonosítja az érintettet, valamint az általa helyesbítésre kért adat nyilvántartás helyét, és gondoskodik az adat helyesbítéséről, ezen eljárása keretében az adat helyesbítésére vonatkozó igényt az ÁKK Zrt. érintett informatikai rendszerének adatgazdája felé jelzi, a szükséges azonosító adatok, a hibás és a helyes adat megadásával. Amennyiben a helyes adat nem áll rendelkezésre, az adatvédelemért felelős személy az érintettől kér felvilágosítást a helyes adatról. Ha a helyes adat nem állapítható meg, az adatvédelemért felelős személy gondoskodik a helytelen adat zárolásáról. A zárolás az adat

passzív állapotba helyezését jelenti, valamint értesíti az érintettet, hogy az adat helyesbítésére a helyes adat hiányában nincs mód, de az adat zárolásra került.

5.5. Adatkezelés korlátozásához való jog

Az érintett jogosult arra, hogy kérésére az ÁKK Zrt. korlátozza az adatkezelést, ha az alábbiak valamelyike teljesül:

- az érintett vitatja a személyes adatok pontosságát, ez esetben a korlátozás arra az időtartamra vonatkozik, amely lehetővé teszi, hogy az ÁKK Zrt. ellenőrizze a személyes adatok pontosságát;
- az adatkezelés jogellenes és az ÁKK Zrt. ellenzi az adatok törlését, és e helyett kéri azok felhasználásának korlátozását;
- az ÁKK Zrt.-nek már nincs szüksége a személyes adatokra adatkezelés céljából, de az érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez;
- az érintett tiltakozott az adatkezelés ellen, de az ÁKK Zrt. jogos érdeke is megalapozhatja az adatkezelést, ebben az esetben, amíg megállapításra nem kerül, hogy az ÁKK Zrt. jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben, az adatkezelést korlátozni kell.

Ha az adatkezelés korlátozás alá esik, az ilyen személyes adatokat a tárolás kivételével csak az érintett hozzájárulásával, vagy jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez, vagy más természetes vagy jogi személy jogainak védelme érdekében, vagy az Európai Unió, illetve valamely tagállam fontos közérdekéből lehet kezelni. Az ÁKK Zrt. az érintettet, akinek a kérésére az adatkezelést korlátozták, az adatkezelés korlátozásának feloldásáról előzetesen tájékoztatja.

5.6. Adathordozhatósághoz való jog

Az adathordozhatóság azt teszi lehetővé, hogy az érintett megszerezhesse és a továbbiakban felhasználhassa az ÁKK Zrt. rendszerében megtalálható általa átadott személyes adatait, saját céljaira és különböző szolgáltatókon keresztül. Minden esetben az érintett által átadott adatokra korlátozódik a jogosultság, egyéb adatok hordozhatóságára lehetőség nincs. (pl. statisztika, tranzakciós adatok stb.).

Az érintett a rá vonatkozó, az ÁKK Zrt. rendszerében megtalálható személyes adatokat:

- tagolt, széles körben használt, géppel olvasható formátumban megkapja,
- jogosult más adatkezelőhöz továbbítani,
- kérheti az adatok közvetlen továbbítását a másik adatkezelőhöz, ha ez technikailag megvalósítható az ÁKK Zrt. rendszereiben.

Az ÁKK Zrt. az adathordozhatóságra vonatkozó kérelmet kizárólag e-mailben vagy postai úton írt kérelem alapján teljesíti. A kérelem teljesítéséhez szükséges, hogy az ÁKK Zrt. meggyőződjön arról, hogy valóban az arra jogosult érintett kíván élni jogával. Ehhez szükséges, hogy az érintett kérelmében megadja azon adatait az ÁKK Zrt. részére, melyet valamely módon megadott részére annak érdekében, hogy tudja azonosítani az igénylő érintettet a rendszerében lévő adatok felhasználásával. Az érintett e jog keretében legfeljebb azon adatok hordozhatóságát igényelheti, melyet önkéntesen megadott az ÁKK Zrt. részére. A jog gyakorlása nem jár automatikusan az adatnak az ÁKK Zrt. rendszereiből való törlésével.

6. Adatkezelés tervezése

Személyes adatok kezelésével járó új tevékenységek megkezdése előtt, az ÁKK Zrt. munkavállalói kötelesek ***10*** *(tíz)* ***munkanappal*** az e Szabályzat 2. számú mellékleteként szereplő minta szerinti adatlapban megjelölt tartalommal az adatkezelési tevékenységet a belső adatvédelemi felelős részére bejelenteni.

Személyes adatok kezelésével járó új tevékenységek megkezdésekor az alábbi feladatokat kell elvégeznie a belső adatvédelemért felelős személynek:

a) meg kell határoznia
   1. a kezelendő személyes adatok körét,
   2. az adatok kezelésének célját,
   3. az adatkezelés jogalapját,
   4. az adatkezelés időtartamát,
b) fel kell mérnie, hogy az adatok milyen informatikai rendszerben lesznek kezelve, az adatok milyen informatikai rendszerben jelennek meg,
c) meg kell határoznia, hogy előre láthatóan az adatokhoz kinek szükséges hozzáférnie az ÁKK Zrt.-n belül, illetve kívül,
d) be kell mutatni, hogy az adatokat szükséges-e továbbítani más személy számára,

e) be kell mutatni, hogy az adatkezeléshez igénybe kell-e venni adatfeldolgozót, amennyiben igen, az adatfeldolgozó feladata mi lesz, várhatóan ki lesz az adatfeldolgozó,
f) meg kell határozni az adatkezelés megkezdésének tervezett időpontját, az adatok felvételének módját és pontos helyét (pl.: erre szolgáló internetes felület vagy papír alapú adatfelvétel).

A kialakított adatkezelési terv alapján az adatkezelésről szóló tájékoztatót és szükség esetén az adatfeldolgozási szerződést, illetve a közös adatkezelési szerződést a belső adatvédelemért felelős személy az adatkezeléssel érintett szakterülettel és a Jogi és Társasági Főosztállyal együttműködésben készíti elő.

7. Adatvédelmi incidensekkel kapcsolatos kötelezettségek és rendelkezések

Az ÁKK Zrt. adatvédelmi incidensekkel kapcsolatos eljárásrendjét a jelen Szabályzat *4. számú melléklete* tartalmazza.

8. Az adatvédelmi tisztviselő/adatvédelmi felelős

Az ÁKK Zrt. adatvédelmi tisztviselőt (DPO –Data Protection Officer), vagy belső adatvédelmi felelőst alkalmaz, ezek kijelölésére a vezérigazgató jogosult.
Az adatvédelmi tisztviselő, illetve a belső adatvédelmi felelős az alábbi feladatokat látja el (amennyiben mindkettő kijelölésre kerül, akkor együttműködésben).
Tájékoztatja és szakmai tanácsot ad a munkáltató és a munkavállalók részére az Általános Adatvédelmi Rendelet (GDPR), valamint az egyéb Európai Uniós és magyarországi adatvédelmi rendelkezések szerinti kötelezettségeikkel kapcsolatban és ennek érdekében:

- ellenőrzi az Általános Adatvédelmi Rendeletnek, valamint az egyéb Európai Uniós és magyarországi adatvédelmi rendelkezéseknek, továbbá a munkáltató személyes adatok védelmével kapcsolatos belső szabályainak való megfelelést, ideértve a feladatkörök kijelölését, az adatkezelési műveletekben résztvevő munkatársak tudatosság-növelését és képzését, valamint a kapcsolódó auditokat is;
- a munkáltató kérésre szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, valamint nyomon követik a hatásvizsgálat elvégzését;

- kivizsgálja a belső adatvédelmi felelős részére érkezett bejelentéseket, és jogosulatlan adatkezelés észlelése esetén annak megszüntetésére hívják fel az ÁKK Zrt.-t, az adatfeldolgozót vagy a közös adatkezelőt;
- vezeti a belső adatvédelmi nyilvántartást;
- gondoskodik az adatvédelmi ismeretek oktatásáról;
- együttműködik az adatvédelmi ügyekért felelős felügyeleti hatósággal, a Nemzeti Adatvédelmi és Információszabadság Hatósággal;
- az adatvédelmi tisztviselő minden, a munkáltató adatkezelésével összefüggő ügyben kapcsolattartó pontként szolgál a felügyeleti hatóság felé, valamint bármely egyéb kérdésben konzultációt folytat vele.

Továbbá jogosult:

- javaslatot tenni az adatvédelmi garanciarendszer kiépítésére,
- javaslatot tenni az adatvédelmi szabályzatok tartalmára,
- adatvédelmi auditot folytathat le,
- közreműködni az adatfeldolgozási és közös adatkezelési szerződések tárgyalásában,
- közreműködni az adatfeldolgozók és közös adatkezelők ellenőrzésében,
- az adatkezelési rendelkezések betartása érdekében általa tett javaslatot - a szakmai irányításáért felelős szervezet általi elfogadása után - az érintett terület vezetője köteles végrehajtani, továbbá erről a belső adatvédelmi felelőst folyamatosan tájékoztatni;
- valamennyi, személyes adat kezelésével foglalkozó terület vezetője tájékoztassa a belső adatvédelmi felelőst arról, milyen javaslatai vannak arra nézve, hogy a személyes adatot milyen strukturált állományban tartsák ill. a hatályos jogszabályokban meghatározott adatkezelési elveket hogyan tudatosítsák,
- értesüljön minden olyan projektről, amely tevékenységét érinti,
- tájékoztatást kapni minden jogellenes adatkezelési, illetve adatfeldolgozási tevékenységről (lásd. adatvédelmi alapelvek).

A belső adatvédelemért felelős személy az adatkezelések átláthatóságának biztosítása érdekében nem nyilvános adatkezelési nyilvántartást vezet, amely tartalmazza legalább:

a) az ÁKK Zrt. kezelésében lévő adatok felsorolását,
b) azt, hogy adott adat milyen informatikai rendszerben kerül kezelésre,
c) az adatok kezelésének és feldolgozásának fizikai helyszínét,

d) annak leírását, hogy az adatok esetleges továbbítása másik adatkezelőhöz, illetve átadása adatfeldolgozók részére milyen módon történik, milyen biztonsági intézkedések mellett,
e) az adathoz milyen típusú munkavállalók vagy megbízottak férhetnek hozzá, ideértve az adatfeldolgozásra jogosult személyeket is,
f) az adat kezelésének mi a jogalapja.

Az adatvédelmi tisztviselő, illetve a belső adatvédelmi felelős az adatkezelést és adatfeldolgozást végző szervezeti egységek munkáját tanácsaival, állásfoglalásaival segíti, valamint az ÁKK Zrt.-nél zajló adatkezelések, adatfeldolgozások törvényességét ellenőrzi. Az egyes adatkezelések, adatfeldolgozások ellenőrzését szükség szerint elvégzi. Az ellenőrzés tapasztalatairól írásban tájékoztatja az ÁKK Zrt. vezérigazgatóját. A szervezeti egységek vezetőitől és munkatársaitól szóban vagy írásban egyaránt felvilágosítást kérhet.

Az adatvédelmi tisztviselőt és a belső adatvédelmi felelőst a vizsgálat során megismert személyes adatokkal kapcsolatban titoktartási kötelezettség terheli.

Jogszabálysértés észlelése esetén az adatvédelmi tisztviselő, illetve a belső adatvédelmi felelős a törvényes állapot helyreállításához segítséget nyújt, ill. amennyiben ez nem kivitelezhető, úgy az adatkezelő munkatársat az adatkezelés megszüntetésére szólíthatja fel.

9. Adattovábbítás

9.1. Általános rendelkezések

Személyes adatok csak akkor továbbíthatók, valamint a különböző adatkezelések akkor kapcsolhatók össze, ha az érintett ahhoz írásban hozzájárult, vagy jogszabály azt megengedi, és ha az adatkezelés feltételei minden egyes személyes adatra nézve teljesülnek. Minden olyan adatkezelésben érintett szakterületnek, amely személyes adatok továbbítását végzi, együtt kell működnie a belső adatvédelmi felelőssel, aki az adattovábbítási nyilvántartást vezeti.

9.2. Adattovábbítás megkeresés alapján

Az ÁKK Zrt.-n kívüli szervezettől vagy magánszemélytől érkező, adatközlésre irányuló megkeresés csak akkor teljesíthető, ha az érintett erre az ÁKK Zrt.-t írásban felhatalmazza. Az érintett előzetesen is adhat ilyen tartalmú felhatalmazást, amely szólhat valamely időtartamra és a megkereséssel élő szervek meghatározott körére. Az adattovábbítás tényét írásban kell

rögzíteni, és az adattovábbítás tényéről az adatvédelmi tisztviselőt, illetve a belső adatvédelmi felelőst tájékoztatni kell.

Az érintett nyilatkozattételétől függetlenül, a vonatkozó jogszabályokban megállapított esetekben teljesíteni kell az illetékes hatóságoktól, állami szervektől, hivataloktól - különösen: rendőrség, bíróság, ügyészség, NAV, TB, valamint a nemzetbiztonsági szolgálatoktól, hagyatéki eljárásban közjegyzőtől stb. - érkezett megkereséseket. Az ilyen megkereséseket az adatkérő általi minősítés szerint kell kezelni, és a megkeresés tényéről az Érintett nem tájékoztatható. E szervek megkereséseiről az illetékes szakterület köteles tájékoztatni a belső adatvédelmi felelőst. A megkeresésekkel kapcsolatos adattovábbítás során a személyes adatra vonatkozó más jogszabályok rendelkezéseit is alkalmazni kell.

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

10.Adatfeldolgozókra vonatkozó általános rendelkezések

Az ÁKK Zrt. mint adatkezelő valamint az általa megbízott adatfeldolgozók a személyes adatok feldolgozásáért, megváltoztatásáért, törléséért, továbbításáért és nyilvánosságra hozataláért felelősek. Az adatfeldolgozó az adatkezelést érintő érdemi döntést nem hozhat, a tudomására jutott személyes adatokat kizárólag az adatkezelő, valamint az adatkezelő és a vele kapcsolatba kerülő ügyfelek és egyéb személyek között fennálló szerződéses viszony rendelkezései szerint dolgozhatja fel, és az ilyen adatokkal saját céljára adatfeldolgozást nem végezhet, a személyes adatokat az Adatkezelő rendelkezései szerint köteles tárolni és megőrizni.

Az adatfeldolgozásra vonatkozó megbízási szerződést írásba kell foglalni. Adatfeldolgozási láncot létrehozni tilos, tehát adatfeldolgozó adatfeldolgozási tevékenységet tovább nem szervezhet ki.
Az adatfeldolgozási szerződésbe bele kell foglalni a feldolgozás időtartamát, lejárta után az adatok visszaszolgáltatásának, vagy feldolgozó oldali törlésének módját.

Adatfeldolgozási szerződés csak EGT-tagállamban, vagy a GDPR-ban foglaltakkal azonos szintű adatvédelemmel rendelkező országban székhellyel rendelkező adatfeldolgozóval köthető. Adattovábbítás is csak ilyen országokból/ba végezhető.

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

Amennyiben az adatkezelő és a megbízott közötti jogviszony adatfeldolgozásra irányul, abban az esetben az adatkezelő felelősségének fenntartásával, az érintett természetes személy (Adatalany) hozzájárulása nélkül - de az adatfeldolgozó igénybevételének tényéről szóló tájékoztatást követően - kerülhet sor az adatok átadására.

A Társaság adatfeldolgozóinak konkrét listáját az adatvedelem@akk.hu e-mail címre írott levélben lehet kérelmezni, amely kérelmeknek az adatkezelő ***30*** *(harminc)* ***napon belül*** írásban tesz eleget, amelyet az adatvédelmi felelős köteles teljesíteni.

11. Az adatfeldolgozói szerződések kötelező tartalmi elemei

A Szabályzat hatálybalépését követően kötött adatfeldolgozói szerződésekben, legalább az alábbiakról kell rendelkezni:

a) szerződés tárgya,
b) az Adatkezelő és az adatfeldolgozó adatai,
c) a feldolgozott adatok körének megjelölése,
d) az adatfeldolgozás céljai,
e) az adatfeldolgozás időtartama,
f) a feldolgozandó személyes adatok becsült mennyisége,
g) az adatfeldolgozó által elvégzett technikai műveletek megnevezése és alapvető elemei;
h) az érintettek köre,
i) adatfeldolgozó által ellátandó feladatok pontos leírása,
j) az utasításhoz kötöttség ténye,
a. a tájékoztatási kötelezettség,

k) azt, hogy az adatfeldolgozó a Rendeletben alkalmazott biztonsági eljárásokra (álnevesítés, titkosítás) felkészül, azokat legkésőbb a Rendelet alkalmazásának megkezdésétől bevezeti;
l) Adatkezelő rendszergazdájának, információbiztonsági felelősének és adatvédelemért felelős személyének elérhetősége,
m) adatfeldolgozó titoktartási kötelezettsége,
n) az adatkezelés jellegének figyelembevételével megfelelő technikai és szervezési intézkedések meghatározása, az adatbiztonsági előírások meghatározása;
o) annak meghatározása, hogy az adatfeldolgozónak az Adatkezelő mely szabályzatainak kell megfelelnie,
p) további adatfeldolgozó igénybevételének lehetőségét, amennyiben ez ismert, a további adatfeldolgozó személyének megjelölésével, amennyiben nem ismert a bevonás menetére vonatkozó rendelkezéseket és az Adatkezelő ellenvetési jogát,
q) a további adatfeldolgozónak megfelelő garanciákat kell nyújtania a megfelelő technikai és szervezési intézkedések végrehajtására, és ezáltal biztosítania kell, hogy az adatkezelés megfeleljen a Rendelet követelményeinek,
r) az adatfeldolgozás befejezését követő eljárásokat (minden személyes adatot törölni kell vagy vissza kell juttatni az Adatkezelő számára és törölni kell a meglévő másolatokat, kivéve, ha az uniós vagy a tagállami jog az személyes adatok tárolását írja elő),
s) a további adatfeldolgozóval az adatfeldolgozónak az eredeti szerződésének megfelelő tartalmú szerződést kell kötnie,
t) az együttműködés elvét azaz, hogy az adatfeldolgozónak kötelessége az Adatkezelővel együttműködni az alanyi jogok teljesítési során,
u) az Adatkezelő és az adatfeldolgozó közötti utasításadás, illetve kapcsolattartás módja,
v) a felelősség elvét, azaz annak tényét, hogy az Adatkezelő az adatfeldolgozó rendelkezésére bocsát minden olyan információt, amely az Adatkezelő Rendeletben megfogalmazott kötelezettségeinek teljesítéséhez szükséges,
w) az audit jog kikötését azaz, hogy az adatfeldolgozó köteles elősegíteni az Adatkezelő által vagy az általa megbízott más természetes vagy jogi személy által végzett auditokat, beleértve a helyszíni ellenőrzéseket,
x) a felelősség egyes kérdései a felek között,
y) jogérvényesítési lehetőségek a felek között.

12. Közérdekű adatok megismerésére irányuló igény és teljesítése

A közérdekű adatok megismerésére irányuló igényre és annak teljesítésére vonatkozó eljárásrendet jelen szabályzat *1. sz. melléklete részletezi*, amelyet az ÁKK Zrt. honlapján is közzé kell tenni.

A közérdekű adatok megismerésére irányuló igény teljesítését a PR és kommunikációs menedzser végzi, az alábbi eljárás szerint:

Az igény teljesítéséért a PR és kommunikációs menedzser felel.

A megismerésre irányuló igényt a beérkezést követő ***24** (huszonnégy)* ***órán belül*** tájékoztatásul meg kell küldeni a Miniszterelnöki Kabinetirodának.

A PR és kommunikációs menedzser az adott adattal rendelkező szakterülettel együttműködve előkészíti az igényre adandó választ és azt a Jogi és Társasági Főosztállyal véleményezteti.

Az előbbiek szerint véglegesített választ döntéshozatalra a vezérigazgató részére elő kell terjeszteni, majd annak döntését követően a Miniszterelnöki Kabinetiroda jóváhagyását be kell szerezni, amelyről a PR és kommunikációs menedzser gondoskodik.

A válasz megküldésére a Miniszterelnöki Kabinetiroda jóváhagyása függvényében és annak megfelelően kerül sor.

13. Személyzeti, bér- és munkaügyi nyilvántartás

13.1. Személyügyi nyilvántartás

A személyügyi nyilvántartás a munkaviszonyra vonatkozó tények dokumentálására szolgáló adatkezelés, melynek alapját a 2012. évi I. törvény (Munka Törvénykönyve), valamint az ÁKK Zrt. *Szervezeti és Működési Szabályzat*a és a Munkaügyi Szabályzata, különösen annak 10. számú melléklete képezi.

A személyügyi nyilvántartás adatai a munkavállaló munkaviszonyával kapcsolatos tények megállapítására, a munkakör betöltéséhez szükséges követelmények igazolására és statisztikai adatszolgáltatásra használhatók fel. Ezen nyilvántartás az ÁKK Zrt.-vel munkaviszonyban álló és időközben kilépett munkavállalók, valamint a természetes személy megbízottai adatait tartalmazza. A személyügyi nyilvántartás adatait az érintett szolgáltatja, a humánpolitikai szakértő és a Főkönyvelőség kezeli vegyes rendszerben, azaz számítógépen és manuális módszerrel. Az elsődleges adatfelvétel a munkaviszony keletkezésekor történik, melyet az ÁKK Zrt. mindenkor hatályos Munkaügyi Szabályzata szabályoz.

A személyügyi nyilvántartásba felvehető adatok az alábbiak:

- név
- születési hely, idő
- anyja neve
- állampolgárság
- személyazonosító igazolvány száma
- TAJ-szám
- adóazonosító jel
- állandó lakcím

- kapcsolattartói, elérhetőségi adatok
- iskolai végzettség
- szakképzettség
- nyelvismeret
- legmagasabb iskolai végzettséget igazoló okirat kelte és száma
- munkaköri leírásban szereplő adatok
- alkalmazási feltételek
- munkabér összege
- munkabér és egyéb juttatás fizetésével kapcsolatos adatok
- erkölcsi bizonyítvány (bemutatásra)
- önéletrajz, motivációs levél és ezekben a munkavállaló által önkéntesen megadásra kerülő további személyes adatok
- munkavállalóra, mint a pályázóra, annak pályázati anyagára vonatkozó következtetést tartalmazó, az ÁKK Zrt. által készített feljegyzés
- munkaviszonyt megszüntető okiratban szereplő adatok
- munkaviszony megszüntetésének napja
- munkaviszony megszüntetésének módja
- tartozások jogcímenként
- értékelésben szereplő adatok (név, munkakör, munkaviszony fennállása, minősítés)

A személyügyi nyilvántartás védelmének módja a következő: az adActa iktatási rendszerben külön Humán iktatókönyv került kialakításra, melyet csak az arra jogosultak érhetnek el (vezérigazgató, vezérigazgató-helyettes, humánpolitikai szakértő, főkönyvelő, adActa rendszer adatgazdája). Az adatok a személyügyi ügykezelést támogató informatikai rendszerben (Kulcs-Bér rendszer) kerülnek tárolásra, amelyben az üzemszerű működés során a humánpolitikai szakértő, illetve a bérszámfejtést végző személy éri el az adatokat, a papír alapon bekért dokumentumokat a humánpolitikai szakértő személyenként dossziéba rendezetten, páncélszekrényben elzárva tárolja. Hibakeresés, vagy más rendellenesség esetén az adott rendszer fejlesztője is hozzáférhet a fenti adatokhoz, amelyre figyelemmel az adott harmadik személy szolgáltatóval megkötendő szolgáltatásra irányuló szerződés megkötése során kell az adatvédelmi szempontokat megfelelően érvényre juttatni.

13.2. Bér- és munkaügyi nyilvántartás

A bér- és munkaügyi nyilvántartás a munkaviszonyra vonatkozó tények dokumentálására szolgáló adatkezelés, melynek alapja a mindenkor hatályos:

- Munka Törvénykönyvéről,
- a társadalombiztosítás ellátásaira és a magánnyugdíjra jogosultakról, valamint e szolgáltatások fedezetéről,
- Számvitelről,
- az adózás rendjéről,
- a személyi jövedelemadóról szóló törvény,
- az ÁKK Zrt. *Szervezeti és Működési Szabályzata,* valamint
- az ÁKK Zrt. *Munkaügyi Szabályzata.*

A bér- és munkaügyi nyilvántartás adatai a munkavállaló munkaviszonyával kapcsolatos tények megállapítására, bérszámfejtésre, adó és társadalombiztosítási ügyintézésre, valamint

statisztikai adatszolgáltatásra használhatók fel. Ezen nyilvántartás valamennyi, az ÁKK Zrt.-vel munkaviszonyban foglalkoztatott munkavállalójának, valamint a természetes személy megbízottjainak adatait tartalmazza.

Ezen nyilvántartást az ÁKK Zrt. a humánpolitikai szakértő és a Főkönyvelősége kezeli vegyes rendszerben, azaz számítógépen és manuális módszerrel.

Az ÁKK Zrt. szervezetén belül a bér- és munkaügyi nyilvántartásból csak a vezérigazgató, valamint azon szervezeti egységek vezetői részére teljesíthető adatszolgáltatás, amelyeknél a munkavállaló a munkaszerződésben meghatározott feladatát végzi.

A bér- és munkaügyi nyilvántartás adatainak feldolgozására adatfeldolgozót megbízni nem lehet.

A személyügyi nyilvántartás adatait - a bér- és bérjellegű adatokat LTO kazettára mentve - tűzálló lemezszekrényben vagy páncélszekrényben, valamint külső banki trezorban elzárva lehet tárolni.

14. E-mail fiók, informatikai eszköz és mobiltelefon használatának ellenőrzésével kapcsolatos adatkezelés

14.1. E-mail fiók használatának ellenőrzésével kapcsolatos adatkezelés

Az ÁKK Zrt. mint munkáltató „céges e-mail fiókot” bocsát a munkavállalók rendelkezésére annak érdekében, hogy a munkavállalók a munkaköri kötelezettségeiket teljesíthessék, ezen keresztül tartsák egymással és harmadik személyekkel a kapcsolatot (az ÁKK Zrt. képviseletében levelezzenek, stb.). Az ÁKK Zrt. hozzájárul ahhoz, hogy a munkavállaló magán célra is használja a céges email címet.

A jelen fejezetben rögzített adatkezelés célja a munkaviszonyból származó kötelezettségek teljesítésének ellenőrzése, jogalapja az Mt. 11-11/A.§-ai.

A „céges e-mail fiók” használatának és ellenőrzésének részletes szabályai az alábbiak:

- a „céges e-mail fiók” használható magáncélokra is, amennyiben a felhasználó úgy használja, hogy a magáncélú levelezését egy Magán vagy Személyes megjelölésű mappában elkülönítve tárolja,
- a magán levelezési mappán keresztül megvalósított levelezés tartalmáért és az adatkezelésért kizárólag a munkavállaló a felelős,

továbbá

- az e-mail fiókról biztonsági másolat készítésének és megőrzésének a szabályozása, az e-mailek végleges törlésének szabályai, valamint az e-mail fiók használatának szabályai, amely utóbbiakat az Informatikai Biztonsági Szabályzat tartalmazza.

A munkáltató évente, valamint a szabályok változása esetén emlékezteti a munkavállalókat arra, hogy milyen előírások vonatkoznak a „céges e-mail fiók” használatára.

Az ÁKK Zrt. mint munkáltató jogosult a „céges e-mail fiók" „személyes"-nek nem minősülő teljes tartalmát és használatát rendszeres időközönként ellenőrizni, amelynek során az adatkezelés alapja a munkáltató jogos érdeke. Az ilyen ellenőrzés célja a munkaköri és egyéb munkavállalói kötelezettségek betartásának ellenőrzése, az e-mailfiók használatára vonatkozó munkáltatói rendelkezések betartásának ellenőrzése.

Amennyiben az ellenőrzés körülményei nem zárják ki ennek lehetőségét, az e-mail fiók használatának ellenőrzése során az ÁKK Zrt. biztosítja a munkavállaló jelenlétét. Ilyen esetben az ellenőrzést megelőzően az ÁKK Zrt. mint munkáltató előzetesen részletes tájékoztatást biztosít a munkavállaló számára, amelyben – az adott eset körülményei alapján indokolt mértékben – tájékoztatja a munkavállalót az alábbiakról:

- milyen célból, milyen munkáltatói érdekek miatt kerülhet sor az e-mail fiók ellenőrzésére;
- a munkáltató részéről ki végzi az ellenőrzést,
- milyen szabályok szerint kerülhet sor ellenőrzésre és mi az eljárás menete,
- milyen jogai és jogorvoslati lehetőségei vannak a munkavállalónak az e-mail fiók ellenőrzésével együtt járó adatkezeléssel kapcsolatban.

Az ellenőrzés során az ÁKK Zrt. mint munkáltató a fokozatosság elvét alkalmazza. Az ellenőrzés első lépéseként az e-mail cím és a levél tárgyának az ellenőrzésére kerül sor, annak megállapítása érdekében, hogy az a munkavállalói munkaköri feladataival kapcsolatos, avagy személyes célú és a Magán vagy Személyes elnevezésű mappában került elhelyezésre. A nem személyes célú leveleket az ÁKK Zrt. mint munkáltató korlátozás nélkül jogosult megismerni és vizsgálni, a személyes célú leveleket az ÁKK Zrt. mint munkáltató viszont – arról való meggyőződésen túl, hogy a vizsgált levél valóban személyes célú vagy sem – nem jogosult megismerni.

Amennyiben megállapításra kerül, hogy a munkavállaló az e-mailfiókot nem a személyes használatra vonatkozó szabályoknak megfelelően használta, felszólításra kerül, hogy a személyes adatokat törölje, illetve az előírtaknak megfelelően tárolja. Ezen esetben az ÁKK Zrt. mint munkáltató a munkavállalóval szemben munkajogi jogkövetkezményeket is alkalmazhat. A munkavállaló távolléte, illetve együttműködésének hiánya esetén az ellenőrzés eredménye alapján az ÁKK Zrt. mint munkáltató törli az érintett adatokat.

A munkavállaló az e-mail fiók ellenőrzésével együtt járó adatkezeléssel kapcsolatban az érintett jogairól szóló rendelkezések szerinti jogorvoslatokkal élhet.

14.2. Számítógép, hordozható számítógép, használatának ellenőrzésével kapcsolatos adatkezelés

Az ÁKK Zrt. mint munkáltató bizonyos munkakörben dolgozó munkavállalók számára a munkavégzés feltételeinek biztosítása érdekében **számítógépet, hordozható számítógépet („céges informatikai eszköz")** biztosíthat a munkájuk elvégzéséhez.

A jelen fejezetben rögzített adatkezelés célja a munkaviszonyból származó kötelezettségek teljesítésének ellenőrzése, jogalapja az Mt. 11-11/A.§-ai.

Amennyiben az ÁKK Zrt. mint munkáltató engedélyezi a hordozható számítógépek esetében a magáncélú használatot, mind az eszközről készített biztonsági mentés során, mind az eszköz

ellenőrzése során az ÁKK Zrt.-nek mint munkáltatónak kiemelt figyelmet kell fordítani arra, hogy a munkavállalók magánélettel kapcsolatos személyes adatait a munkáltató nem kezelheti.

Amennyiben az ÁKK Zrt. mint munkáltató a munkavállalók számára a „céges e-mail fiók" magáncélú használatát is lehetővé teszi és a munkavállaló azt a céges informatikai eszközön ilyen célra használja, úgy az ezen használatra a céges e-mailfiók használatra vonatkozó szabályok értelemszerűen irányadóak.

A „céges informatikai eszköz" használatának és ellenőrzésének részletes szabályai az alábbiak:

- Amennyiben az ellenőrzés körülményei nem zárják ki ennek lehetőségét, a céges informatikai eszközök (pl. laptop, asztali munkaállomás) használatának ellenőrzése során az ÁKK Zrt. biztosítja a munkavállaló jelenlétét. Ilyen esetben az ellenőrzést megelőzően az ÁKK Zrt. mint munkáltató előzetesen részletes tájékoztatást biztosít a munkavállaló számára, amelyben – az adott eset körülményei alapján indokolt mértékben – tájékoztatja a munkavállalót az alábbiakról:
    - milyen célból, milyen munkáltatói érdekek miatt kerülhet sor az ellenőrzésre;
    - a munkáltató részéről ki végzi az ellenőrzést,
    - milyen szabályok szerint kerülhet sor ellenőrzésre és mi az eljárás menete,
    - milyen jogai és jogorvoslati lehetőségei vannak a munkavállalónak a „céges informatikai eszköz" ellenőrzésével együtt járó adatkezeléssel kapcsolatban.

Az ellenőrzés során az ÁKK Zrt. mint munkáltató a fokozatosság elvét alkalmazza. Ezen túlmenően a munkáltatói ellenőrzést is úgy kell a munkáltatónak végrehajtania, hogy az ellenőrzés ne érintse a céges informatikai eszközön esetlegesen található személyes adatokat, azokat az ellenőrzéssel összefüggésben nem tárolhatja.

14.3. Mobiltelefonok és tabletek használatának ellenőrzésével kapcsolatos adatkezelés

Az ÁKK Zrt. mint munkáltató bizonyos munkakörben dolgozó munkavállalók számára „céges mobiltelefont és tabletet " biztosít a munkájuk elvégzéséhez, melyek esetében a magáncélú használatot az ÁKK Zrt. engedélyezi. A céges levelezést ezen eszközökön, amennyiben azt az eszköz támogatja, kizárólag biztonságos „konténerizált" környezetben lehet igénybe venni, elérni. Amennyiben az eszköz nem támogatja ezt a megoldást, úgy fokozott figyelemmel kell eljárni annak érdekében, hogy az eszközön megfelelő jelszóval feloldható időkorlát kerüljön beállításra az illetéktelen hozzáférés elkerülése érdekében.

A jelen fejezetben rögzített adatkezelés célja a munkaviszonyból származó kötelezettségek teljesítésének ellenőrzése, jogalapja az Mt. 11-11/A.§-ai.

Az ÁKK Zrt. mint munkáltató a munkavállalók számára a „céges e-mail fiók" magáncélú használatát is lehetővé teszi és a munkavállaló azt a céges mobiltelefonon és tableten ilyen célra használja, úgy az ezen használatra a céges e-mailfiók használatra vonatkozó szabályok értelemszerűen irányadóak.

A „céges mobiltelefonok" használatának és ellenőrzésének részletes szabályai az alábbiak:

- Az ellenőrzést megelőzően az ÁKK Zrt. mint munkáltató előzetesen részletes tájékoztatást biztosít a munkavállaló számára, amelyben – az adott eset körülményei alapján indokolt mértékben – tájékoztatja a munkavállalót az alábbiakról:
    - milyen célból, milyen munkáltatói érdekek miatt kerülhet sor az ellenőrzésre;
    - a munkáltató részéről ki végzi az ellenőrzést,
    - milyen szabályok szerint kerülhet sor ellenőrzésre és mi az eljárás menete,
    - milyen jogai és jogorvoslati lehetőségei vannak a munkavállalónak a „céges mobiltelefon” ellenőrzésével együtt járó adatkezeléssel kapcsolatban.

Az ellenőrzés során az ÁKK Zrt. mint munkáltató a fokozatosság elvét alkalmazza. Ezen túlmenően a munkáltatói ellenőrzést is úgy kell a munkáltatónak végrehajtania, hogy az ellenőrzés ne érintse a telefonon található személyes adatokat, azokat az ellenőrzéssel összefüggésben nem tárolhatja.

15. Adótitok körébe tartozó adatok kezelése és védelme

Az adótitok körébe tartozó adatokat harmadik személy elől el kell zárni. Az informatikai rendszerekben (adActa iktatórendszer, Kulcs-Soft programok) ezen adatokhoz kizárólag azon munkavállalók férnek hozzá, akik adóadatokkal foglalkoznak. A dedikált munkaállomások rendszeresen mentésre kerülnek. A papír alapú dokumentumokat a kijelölt szakértő tárolja elzártan. A Kulcs-Soft programok esetében külön felhasználónév és jelszó került beállításra, függetlenül a tartományi bejelentkezéshez használtaktól.

Az ÁKK Zrt. azon munkavállalói, akik munkavégzésük során adóadatokat dolgoznak fel, adó és adóelőleg levonását végzik, valamint akik adózást érintő adótitok birtokába kerülnek, kötelesek az adótitok megőrzésére.

Az adótitok körébe tartozó adatok kezelésével, illetve védelmével kapcsolatosan az alábbiakban felsorolt mindenkor hatályos jogszabályok rendelkezései irányadóak:

1. az információs önrendelkezési jogról és az információszabadságról szóló törvény
2. az adózás rendjéről szóló törvény.

16. Banktitok körébe tartozó adatok kezelése és védelme

Az ÁKK Zrt. azon munkavállalója, aki banktitok birtokába jut, nem használhatja fel arra, hogy annak révén saját maga vagy más személy részére közvetlen vagy közvetett módon előnyt szerezzen, továbbá, hogy a pénzügyi intézménynek vagy az intézmény ügyfeleinek hátrányt okozzon, valamint köteles azt időbeli korlátozás nélkül megtartani.

A banktitok körébe tartozó adatok kezelésével, illetve védelmével kapcsolatosan az alábbiakban felsorolt mindenkor hatályos jogszabályok rendelkezései irányadóak:

1. az információs önrendelkezési jogról és az információszabadságról szóló törvény,
2. a hitelintézetekről és a pénzügyi vállalkozásokról,
3. a pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról.

17. Értékpapírtitok körébe tartozó adatok kezelése és védelme

Az ÁKK Zrt. azon munkavállalója, akinek értékpapírtitok birtokába jut, köteles azt – törvény eltérő rendelkezésének hiányában - időbeli korlátozás nélkül megtartani.

Az ÁKK Zrt. azon munkavállalója, aki értékpapírtitok birtokába jut, azt nem használhatja fel arra, hogy annak révén saját maga vagy más személy részére közvetlen vagy közvetett módon előnyt szerezzen.

A titoktartási kötelezettség alapján az értékpapírtitok körébe tartozó tény, információ, megoldás vagy adat a Bszt-ben meghatározott körön kívül – az ügyfél felhatalmazása nélkül - nem adatható ki harmadik személynek és feladatkörön kívül nem használható fel.

Az értékpapírtitok körébe tartozó adatok kezelésével, illetve védelmével kapcsolatosan az alábbiakban felsorolt mindenkor hatályos jogszabályok rendelkezései irányadóak:

1. az információs önrendelkezési jogról és az információszabadságról szóló törvény,
2. a befektetési vállalkozásokról és az árutőzsdei szolgáltatókról, valamint az általuk végezhető tevékenységek szabályairól szóló törvény.

18.A minősített adat kezelése és védelme

A Bizalmas minősítésű, a Titkos minősítésű és a Szigorúan titkos minősítésű adatok kezelését és védelmét az ÁKK Zrt. mindenkor hatályos *titkos ügyiratkezelés rendjéről szóló szabályzat*a szabályozza.

19.A társasági iratok személyes adatainak kezelése és védelme

Az ÁKK Zrt. mint gazdasági társaság működésére, a cégnyilvántartásra, a cégnyilvánosságra, valamint a Cégnyilvántartásban nyilvántartott dokumentumokban szereplő személyes adatokra vonatkozóan az alábbiakban felsorolt mindenkor hatályos törvények rendelkezései irányadóak:

1. a Polgári Törvénykönyvről szóló törvény (a továbbiakban: Ptk.),
2. a cégnyilvántartásról, a cégnyilvánosságról és a bírósági cégeljárásról szóló törvény.

20.Üzleti titok körébe tartozó adatok kezelése és védelme

Jogszabály, vagy belső szabályzat kifejezett eltérő rendelkezés hiányában az ÁKK Zrt.-nél keletkezett valamennyi olyan információ, amely az ÁKK Zrt. Stabilitási törvényben, illetve államháztartásról szóló 2011. évi CXCV. törvényben meghatározott tevékenységét érinti, az az ÁKK Zrt. üzleti titkának minősül függetlenül attól, hogy az szóbeli, írott vagy számítástechnikai adat.

Az ÁKK Zrt. azon munkavállalója, aki üzleti titok birtokába jut köteles azt időbeli korlátozás nélkül megtartani, az üzleti titkot engedély nélkül nem hozhatja nyilvánosságra, harmadik személynek nem szolgáltathatja ki, és azt kizárólag az ÁKK Zrt. tevékenységével és működésével kapcsolatban azzal összhangban használhatja fel és hasznosíthatja, nem használhatja fel arra, hogy annak révén saját maga vagy más személy részére közvetlen vagy közvetett módon előnyt szerezzen, vagy az ÁKK Zrt.-nek hátrányt vagy kárt okozzon! Amennyiben pedig ennek ellenére az adott információ jogosulatlan kezeléséről, illetve felhasználásáról szerez tudomást, úgy arról köteles a szervezeti egység vezetőjét értesíteni.

A fentiek megszegése vagy be nem tartása munkajogi, polgári jogi és büntetőjogi jogkövetkezményekkel járhat.

Amennyiben jogszabály közérdekből elrendeli valamely az ÁKK Zrt.-nél keletkező adat nyilvánosságra hozatalát az ilyen nyilvánosságra hozatal nem eredményezheti az olyan adatokhoz való hozzáférést, amelyek megismerése az üzleti tevékenység végzése szempontjából aránytalan sérelmet okozna, feltéve, hogy ez nem akadályozza meg a közérdekből nyilvános adat megismerésének lehetőségét.

A vezérigazgató, a megbízott ügyvédek, a jogtanácsosok, a belső ellenőr és a Beszerzési és ellátási főosztály vezetője betekinthetnek bármely szervezeti egységnél készített anyagba. Ez a jogosultság – Ptk.-ben foglaltak alapján - megilleti az ÁKK Zrt. Igazgatóságának és Felügyelő Bizottságának tagjait is.

Az üzleti titok körébe tartozó adatok kezelésével, illetve védelmével kapcsolatosan az alábbiakban felsorolt jogszabályok rendelkezései irányadóak:

1. 2018. évi LIV. törvény az üzleti titok védelméről,
2. 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról,
3. 2013. évi V. törvény a Polgári Törvénykönyvről.

21. „Szigorúan bizalmas!" adatokat tartalmazó dokumentumok minősítése

Amennyiben az érintett üzleti titok fokozott védelmet igényel és az irat keletkeztetője úgy ítéli meg, hogy **„Szigorúan bizalmas!"** iratként kell kezelni az általa elkészített iratot, kezdeményezi minősítését az *3. számú melléklet* szerinti „Minősítési javaslat" benyújtásával.

Az ÁKK Zrt.-nél üzleti titkok körében minősítési jogkörrel kizárólag a vezérigazgató rendelkezik.

A minősítést kezdeményezheti:

- az ÁKK Zrt. szervezeti egységeinek vezetői,
- az ÁKK Zrt. jogtanácsosa,
- a belső ellenőr.

22. A „Szigorúan bizalmas!" jelzéssel minősített dokumentumok készítése, kezelése és védelme

A „Szigorúan bizalmas!" jelzéssel minősített iratokat az alábbi formai követelményeknek megfelelően kell elkészíteni.

A minősített irat fedőlapjának tartalmaznia kell az alábbi adatokat:

- a készítő szervezeti egység neve,
- a készítő neve,
- a begépelő neve (amennyiben nem egyezik meg a készítő nevével),
- a minősítés fajtája,
- a minősítő neve,
- a minősítés időtartama dátum szerint,
- mennyi eredeti és mennyi másolati példány készült,
- név szerint kihez kerültek a számozott példányok,
- az irat iktatási száma.

A minősített irat minden oldalán fel kell tüntetni a minősítés tényét, azaz minden oldalt el kell látni „Szigorúan bizalmas!” felirattal.

A minősítő személynek meg kell határozni, hogy milyen időtartamra szól a minősítés, melyet a minősített iraton minden esetben fel kell tüntetni. A minősítés időtartamát kizárólag az iratot elsődlegesen minősítő személy módosíthatja.

Az irat iktatása (elektronikus iktatás) során biztosítani kell, hogy a rendszerben csak az arra illetékes személyek tudják elérni az adatokat. Az iktatás során ezen anyagok szkennelése, másolása, sokszorítása **TILOS**.

Minősített iratokat kézbesíteni kizárólag zárt borítékban lehet, melyen fel kell tüntetni a „Saját kezű felbontásra!” megjelölést, a minősítés megnevezését, valamint az irat iktatási számát. Az ilyen módon megcímzett borítékot csak a címzett bonthatja fel, abban az esetben, ha a címzett nem elérhető, ezen küldeményt csak a címzett helyettesítésére kijelölt személy vagy az ÁKK Zrt. vezérigazgatója bonthatja ki.

Minősített iratot elektronikusan kizárólag tömörített és jelszóval védett formában lehet továbbítani, melyhez a jelszót külön levélben kell megküldeni, melynek tárgyában nem szerepelhet a jelszó szó vagy a jelszóra utaló szövegrész.

A „Szigorúan bizalmas!” minősítéssel ellátott anyagokat a többi anyagtól elkülönítetten kell tárolni.

A minősített iratok megsemmisítésére kizárólag a minősítés érvényességi idejének lejáratát követően kerülhet sor az ÁKK Zrt. mindenkor hatályos Iratkezelési Szabályzata szerint.

23.Vonatkozó jogszabályok

A jelen szabályzatban nem szabályozott esetekben a vonatkozó jogszabályok rendelkezései irányadóak (a legfontosabbakat az 5. számú melléklet összesíti).

Mellékletek

1. számú melléklet - A közérdekű adatok megismerésére irányuló igényre és annak teljesítésére vonatkozó eljárásrend

Az ÁKK Zrt. vezérigazgatója az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (továbbiakban: Info tv.) 30. § (6) bekezdésére és a közérdekű adat iránti igény teljesítéséért megállapítható költségtérítés mértékéről szóló 301/2016 (IX.30.) Korm. rendeletre tekintettel az ÁKK Zrt. által teljesítendő közérdekű adatok megismerésére irányuló igényre és annak teljesítésére vonatkozó szabályokat a következők szerint állapítja meg:

1. Ezen eljárásrend szerinti szabályokat kell alkalmazni az ÁKK Zrt. kezelésében lévő közérdekű adatok, közérdekből nyilvános adatok (a továbbiakban együtt: közérdekű adat) megismerésére irányuló igényekre és azok teljesítésére.
2. A közérdekű adat megismerése iránt az ÁKK Zrt.-nél szóban és írásban (levélben vagy elektronikus úton) bárki igényt nyújthat be. A beérkezett igényt az ÁKK Zrt. nyilvántartásba veszi.
3. Az adatigénylésnek az ÁKK Zrt. nem köteles eleget tenni, ha az igénylő nem adja meg nevét, nem természetes személy igénylő esetén megnevezését, valamint azt az elérhetőséget, amelyen számára az adatigényléssel kapcsolatos bármely tájékoztatás és értesítés megadható.
4. A közérdekű adat megismerésére irányuló igénynek az ÁKK Zrt. az igény tudomására jutását követő legrövidebb idő alatt, legfeljebb azonban ***15 (tizenöt) napon belül*** tesz eleget, ez a határidő egy alkalommal az Info tv-ben meghatározott esetben ***15 (tizenöt) nappal*** meghosszabbítható. Amennyiben az ÁKK Zrt. a lentebb részletezett szabályok szerint költségtérítést állapít meg, az adatigénylést a költségtérítésnek az igénylő általi megfizetését követő ***15 (tizenöt) napon belül*** kell teljesíteni.
5. Az adatigénylésnek közérthető formában és - amennyiben azt az ÁKK Zrt. aránytalan nehézség nélkül teljesíteni képes - az igénylő által kívánt formában, illetve módon kell eleget tenni. Ha a kért adatot korábban már elektronikus formában nyilvánosságra hozták, az igény teljesíthető az adatot tartalmazó nyilvános forrás megjelölésével is. Az adatigénylést nem lehet elutasítani arra való hivatkozással, hogy annak közérthető formában nem lehet eleget tenni.
6. A szóban előterjesztett igényt akkor lehet szóban teljesíteni, ha az igénylő szóban kéri a választ, illetve az számára kielégítő és
    a. az igényelt adat az ÁKK Zrt. honlapján vagy más módon jogszerűen már nyilvánosságra került; vagy
    b. az igény az ÁKK Zrt. hatáskörére, eljárására, az alkalmazott jogszabályokra vonatkozó általános tájékoztatással teljesíthető.
7. A 6. pont szerinti igény szóbeli teljesítésére az ÁKK Zrt. bármelyik munkavállalója jogosult. Az igény szóbeli teljesítéséről, valamint a szóban meg nem válaszolható igényekről feljegyzést kell készíteni. Az igénylőt egyidejűleg tájékoztatni kell arról, hogy igényének teljesítésére írásban kerül sor. Az igény írásbeli teljesítése érdekében fel kell venni az igénylő elérhetőségét (elektronikuslevél-címét, postai elérhetőségét vagy telefaxszámát).
8. Közérdekű adat iránti igényt írásban elsősorban az ÁKK Zrt. postai címén (1253 Budapest, Pf. 85), elektronikus levélcímén (kozerdekuigeny@akk.hu), faxszámán

(06 1 488-9405), továbbá az ÁKK Zrt. honlapjának (www.akk.hu) e célra kialakított részén (a https://akk.hu/contact link alatt, az – Általános menüpontot választva) lehet benyújtani.

9. Ha törvény másként nem rendelkezik, az ÁKK Zrt. az adatigénylő személyes adatait csak annyiban kezeli, amennyiben az az igény teljesítéséhez, az igénynek az Info tv. 29.§ (1a) bekezdésében meghatározott szempont alapján való vizsgálatához, illetve az igény teljesítéséért megállapított költségtérítés megfizetéséhez szükséges. Az Info tv. 29. § (1a) bekezdésében meghatározott ***1 (egy) év leteltét***, illetőleg a költségek megfizetését követően, az ÁKK Zrt. az adatigénylő személyes adatait haladéktalanul törli. Az ÁKK Zrt. az adatigénylő személyes adatainak kezeléséről szóló adatkezelési tájékoztatóját az igénylő részére legkésőbb az adatigénylésre adott válaszával egyidejűleg küldi meg.

10. Ha a közérdekű adatigénylés alapján megállapítható, hogy az igényelt adatokat vagy azok egy részét nem az ÁKK Zrt. kezeli, úgy az igényt az ÁKK Zrt. az illetékes szervhez ***3 (három) munkanapon belül*** átadja az igénylő egyidejű írásbeli értesítése mellett.

11. Az igényelt közérdekű adatot tartalmazó dokumentumról vagy dokumentumrészről, annak tárolási módjától függetlenül, az igénylő másolatot kaphat. Az ÁKK Zrt. az adatigénylés teljesítéséért[10] – az *1. függelék* szerint, az Info tv., valamint a közérdekű adat iránti igény teljesítéséért megállapítható költségtérítés mértékéről szóló 301/2016. (IX. 30.) Korm. rendelet (a továbbiakban: Korm. rendelet) figyelembevételével – legfeljebb a felmerült költségek mértékéig terjedően költségtérítést állapíthat meg, akkor, ha a felmerült költség mértéke meghaladja a Korm. rendeletben meghatározott, költségtérítésként megállapítható legalacsonyabb összeget, azzal, hogy az így meghatározott költségtérítés összege ekkor sem haladhatja meg a Korm. rendeletben meghatározott legmagasabb összeget. A költségtérítés összegéről, a költség megfizetésének módjáról, valamint az adatigénylés teljesítésének a másolatkészítést nem igénylő lehetőségeiről az igénylőt az igény beérkezését követő ***15 (tizenöt) napon belül*** tájékoztatni kell.

12. Az igénylő a 10. pont alapján kapott tájékoztatás kézhezvételét követő ***30 (harminc) napon belül*** nyilatkozik arról, hogy az igénylését fenntartja-e. A tájékoztatás megtételétől az igénylő nyilatkozatának az adatkezelőhöz való beérkezéséig terjedő időtartam az adatigénylés teljesítésére rendelkezésre álló határidőbe nem számít bele. Ha az igénylő az igényét fenntartja, a *2. számú függelék* szerinti költségtérítést az ÁKK Zrt. által megállapított, legalább ***15 (tizenöt) napos*** határidőben köteles az ÁKK Zrt. részére megfizetni.

13. A költségtérítés történhet személyes átvétel esetén egyidejű befizetéssel, átutalással, postai úton történő átvétel esetén postai utánvét útján.

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

15. Az igény teljesítésének megtagadásáról, annak indokaival és az Info tv. alapján megillető jogorvoslati lehetőségekről való tájékoztatással együtt, ***15 (tizenöt) napon belül*** írásban vagy – amennyiben az igényben elektronikuslevél-címét közölte – elektronikus úton értesíteni kell az igénylőt. Az elutasított kérelmekről, valamint az

[10] Elektronikus úton előterjesztett adatigényléseket az ÁKK Zrt elsődlegesen e-mail útján teljesíti, kifejezett kérés esetén, illetve ha az e-mail-en történő továbbítást az igényelt közérdekű adatok fájlmérete nem teszi lehetővé, sor kerülhet adathordozón történő teljesítésre.

elutasítások indokáról az ÁKK Zrt-nek minden év január 31-éig tájékoztatnia kell az Nemzeti Adatvédelmi és Információszabadság Hatóságot.

A közérdekű adat megismerése iránti igény teljesítése nem tagadható meg azért, mert a nem magyar anyanyelvű igénylő az igényét anyanyelvén vagy az általa értett más nyelven fogalmazza meg.

16. Az igénylő a közérdekű adat megismerésére vonatkozó igény elutasítása vagy a teljesítésre nyitva álló (illetve a meghosszabbított) határidő eredménytelen eltelte esetén, valamint az adatigénylés teljesítéséért megállapított költségtérítés összegének felülvizsgálata érdekében a Fővárosi Törvényszéken keresettel élhet.
17. Az adatigénylő a közérdekű adatok megismeréséhez fűződő jogok gyakorlásával kapcsolatos jogsértés esetén a Nemzeti Adatvédelmi és Információszabadság Hatósághoz is fordulhat.
18. A 16. pont szerinti pert az igény elutasításának közlésétől, a határidő eredménytelen elteltétől, illetve a költségtérítés megfizetésére vonatkozó határidő lejártától számított harminc napon belül kell megindítani. Ha az igény elutasítása, nem teljesítése vagy az adatigénylés teljesítéséért megállapított költségtérítés összege miatt az igénylő a Nemzeti Adatvédelmi és Információszabadság Hatóságnál bejelentést tesz, a pert a bejelentés érdemi vizsgálatának elutasításáról, a vizsgálat megszüntetéséről, vagy lezárásáról, továbbá az adatkezelő jogsérelem orvoslására, illetve annak közvetlen veszélye megszüntetésére történő felszólítása eredményéről szóló értesítés kézhezvételét követő harminc napon belül lehet megindítani.

1. számú
függelék

Az ÁKK Zrt. által
a közérdekű adat iránti igény teljesítéséért megállapításra kerülő
költségtérítés mértéke

1. A/4-es oldal másolása (fekete-fehér): 12,00 Ft/oldal
A/3-as oldal másolása (fekete-fehér): 24,00 Ft/oldal
2. A/4-es oldal másolása (színes): 130,00 Ft/oldal
A/3-as oldal másolása (színes): 260,00 Ft/oldal
3. optikai adathordozón nyújtott másolat (CD lemeze, DVD lemez, stb.): 580 Ft/adathordozó
5. elektronikus úton használható egyéb adathordozón nyújtott másolat: közvetlen önköltség
6. Kézbesítés díja: Korm. rendelet szerint

Az 1-2. pont alatti költség a másolt oldalak azon része tekintetében kerül érvényesítésre, amellyel a másolt oldalak száma a tízet meghaladja.

2. számú melléklet – Új adatkezelés bejelentésének tartalma

SORSZÁM	ADATKEZELÉSI TEVÉKENYSÉG MEGNEVEZÉSE	ADATKEZELŐ/KÖZÖS ADATKEZELŐ NEVE, ELÉRHETŐSÉGE, KÉPVISELŐJE (30.cikk (1) a pont)	ADATKEZELÉS CÉLJA (30.cikk (1) b pont)	ÉRINTETTEK KATEGÓRIÁI (30.cikk (1) c pont)	SZEMÉLYES ADATOK KATEGÓRIÁI (30.cikk (1) c pont)	ADATKEZELÉS JOGALAPJA	CÍMZETTEK (30.cikk (1) d pont)	ADATTOVÁBBÍTÁS	ADATTOVÁBBÍTÁS HARMADIK ORSZÁGNAK, NEMZETKÖZI SZERVEZETHEZ (30.cikk (1) e pont)	HARMADIK ORSZÁGBA TÖRTÉNŐ TOVÁBBÍTÁS INFORMÁCIÓI (30.cikk (1) e pont)	AZ ADATKATEGÓRIÁK TÖRLÉSÉRE ELŐIRÁNYZOTT HATÁRIDŐ (30.cikk (1) f pont)	TECHNIKAI ÉS SZERVEZÉSI INTÉZKEDÉSEK ÁLT. LEÍRÁSA (30.cikk (1) g pont)
1												
2												
3												
4												
5												
6												
7												
8												
9												
10												
11												
12												
13												
14												
15												
16												
17												
18												
19												

3. számú melléklet - Minősítési javaslat

Minősítési javaslat

A …… Iktató számú ……tárgyú üzleti titkot tartalmazó irat a minősítés formai követelményeinek megfelelő formában ezen javaslat melléklete.

A fenti információt javaslom ……évre,……év……..hó …….. napjáig „Szigorúan bizalmas!" –nak minősíteni.

Indoklás

A „Szigorúan bizalmas!" minősítés indokolt, mivel ……
……
……
……

Budapest, ……..

……..
a minősítés kezdeményezőjének aláírása

……
a minősítés kezdeményezőjének neve

……
a minősítés kezdeményezőjének
szervezeti egysége

Az irat „Szigorúan bizalmas!" minősítését engedélyezem/ nem engedélyezem*.

……..
a minősítő aláírása

……
a minősítő neve

* A megfelelő szövegrész aláhúzandó!

4. számú melléklet - Az ÁKK Zrt. adatvédelmi incidensekkel kapcsolatos eljárásrendje

I. Általános rendelkezések
1. Az eljárásrend hatálya

II. Az adatvédelmi incidens
1. Az adatvédelmi incidens fogalma, jellemzői
2. Az incidensek fajtái
   - 2.1 Megsemmisítés
   - 2.2 Személyes adatok elvesztése
   - 2.3 Megváltoztatás
   - 2.4 Jogosulatlan közlés
   - 2.5 Jogosulatlan hozzáférés
3. A nem bejelentésköteles, „bagatell" incidensek
4. Az incidensek nyilvántartása

III. Részletes rendelkezések
1. Az adatvédelmet sértő események kezelési rendjének célja, tartalma
2. Az adatvédelmet sértő események megelőzésével és kezelésével kapcsolatos felelősségek
3. A vezető munkatársak alapvető kötelezettségei
4. Az adatvédelmet sértő esemény észlelése, feltárása, bejelentése
5. Az adatvédelmet sértő esemény megszüntetésére tett intézkedések
6. Jogkövetkezmények alkalmazása
7. Az adatvédelmet sértő eseményekkel kapcsolatos intézkedések, eljárások nyomon követése
8. Adatvédelmi hatásvizsgálat

I. ÁLTALÁNOS RENDELKEZÉSEK

Az ÁKK Zrt., mint Adatkezelő tiszteletben tartja mindazon személyek magánszféráját, akik számára személyes adatot adnak át és elkötelezett ezek védelmében. Az Európai Unió Általános Adatvédelmi Rendelet (679/2016 sz. rendelet, a továbbiakban: GDPR) (88) preambulum-bekezdése alapján az alábbi eljárásrendet alkotja:

1. Az eljárásrend hatálya

Az ÁKK Zrt. működése során bekövetkező adatvédelmi incidens kezelésére az alábbi eljárásrendet kell alkalmazni.

2. **Az itt használt fogalmak** a szabályzatban meghatározott jelentéssel bírnak.

II. Az adatvédelmi incidens

1. Az adatvédelmi incidens fogalma, jellemzői

Adatvédelmi incidens alatt a biztonság olyan sérülését kell érteni, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi.

Az adatvédelmi incidens megfelelő és kellő idejű intézkedés hiányában fizikai, vagyoni vagy nem vagyoni károkat okozhat a természetes személyeknek (többek között a személyes adataik feletti rendelkezés elvesztését vagy a jogaik korlátozását, a hátrányos megkülönböztetést, a személyazonosság-lopást vagy a személyazonossággal való visszaélést, a pénzügyi veszteséget, az álnevesítés engedély nélküli feloldását, a jó hírnév sérelmét, a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülését, illetve a szóban forgó természetes személyeket sújtó egyéb jelentős gazdasági vagy szociális hátrányt).

Az ÁKK Zrt.-nél az incidensek kezelésére hatáskörrel rendelkező szervezeti egységek vezetői:

- Jogi és Társasági Főosztály vezetője / adatvédelemért felelős személy/ adatvédelem és adatkezelés koordinálásáért felelős szakterület
- Informatikai Főosztály vezetője / informatikai biztonsági felelős/ adatbiztonságért felelős szakterület.

2. Az incidensek fajtái

2.1 Megsemmisítés

Ha akár az adathordozó maga, akár a személyes adatok helyreállíthatósága szűnik meg, visszaállíthatatlan módon.

2.2 Személyes adatok elvesztése

Ha az adat nem semmisül meg ugyan, de kikerül az adatkezelő, vagy adatfeldolgozó rendelkezése alól, pl. elvész, vagy ellopják, ill. ha maga a titkosítási kulcs vész el, vagy lopják el azt.

2.3 Megváltoztatás

Nem minden megváltoztatás incidens, csak az, ami olyan változást jelent, amely nem az érintett kérésére, ill. nem egy másik alapelv (a pontosság követelménye) miatt történik. A változtatásnak pedig szükségszerűen véletlennek, vagy jogellenesnek kell lennie.

2.4 Jogosulatlan közlés

Az adat véletlenszerű, vagy jogellenes továbbítása olyan harmadik személyhez, aki semmilyen más jogszabály, vagy jogviszony alapján nem jogosult a megismerésre.

2.5 Jogosulatlan hozzáférés

Ha a biztonsági sérülés miatt harmadik személy jogosulatlanul fér hozzá az adatokhoz (pl. belső szabályzat megszegése, vagy a biztonsági intézkedések szándékos kijátszása esetén).

3. A nem bejelentésköteles, „bagatell" incidensek

Nem szükséges bejelenteni a felügyeleti hatóságnak azt az incidenst, amely valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Ilyen pl. egy rossz helyre küldött email (jogosulatlan hozzáférés), amelyet azonban a hozzáférő azonnal töröl és ezt írásban visszaigazolja.

4. Az incidensek nyilvántartása

Az ÁKK Zrt., mint Adatkezelő, minden incidenst belső nyilvántartásba vesz a GDPR 33. cikk (5) bekezdése szerinti tartalommal. Ennek megfelelően nyilvántartja az incidensek okait, a történéseket és az érintett személyes adatok körét, valamint az incidensek hatásait és következményeit, továbbá az orvoslásukra tett intézkedéseket. Megőrzési határidő azonos az elszámoltathatóság elvére figyelemmel azzal a határidővel, amíg a hatóság számon kérheti az ÁKK Zrt.-t a bizonyítékok átadására, vagy valamely esetlegesen jogellenes adatkezelés felgöngyölítésére.

A nyilvántartás vezetéséről az adatvédelmi felelős köteles gondoskodni.

III. RÉSZLETES RENDELKEZÉSEK

1. Az adatvédelmet sértő események kezelési rendjének célja, tartalma

Az eljárásrend célja annak elősegítése, hogy az ÁKK Zrt. működésével kapcsolatosan felmerülő adatvédelmet sértő események kezelése egységes rendszerben történjen, kialakulásának megelőzésére, a bekövetkezése esetében annak feltárására, szükség esetén a felelősség megállapítására, intézkedések megtételére sor kerüljön. Az eljárásrend ennek érdekében rögzíti azokat a fogalmakat, eljárásokat, intézkedéseket, amelyek biztosítják az ÁKK Zrt. működése során előforduló, adatvédelmet sértő esemény ismételt előfordulásának megelőzését, és a feltárt események kezelését.

2. Az adatvédelmet sértő események megelőzésével és kezelésével kapcsolatos felelősségek

Az adatvédelmet sértő események megelőzése és kezelése (az eljárásrend kialakítása, a szükséges intézkedések meghozatala) az ÁKK Zrt. felelőssége, melynek e felelőssége és feladata a szervezeti struktúrában meghatározott szervezeti egységek vezetői hatáskörének, felelősségének és beszámoltathatóságának szabályozottságán keresztül valósul meg.

3. Ennek érdekében a vezető munkatársak alapvető kötelezettsége, hogy

a) a jogszabályoknak megfelelő szabályozások alapján működjön a szervezet, és ennek érdekében a szükséges, feladatkörükhöz tartozó szabályozások előkészítésre kerüljenek,
b) a szabályozottságot, valamint a szabályok betartását minden vezető folyamatosan kísérje figyelemmel, amely elsődleges feltétele az adatvédelmet sértő események megelőzésének,
c) adatvédelmet sértő esemény észlelése esetén minél gyorsabban kellően hatékony intézkedés történjen annak érdekében, hogy az adatvédelmet sértő esemény megszüntetésre, az esetleges hibás belső szabályozás helyesbítésre kerüljön,
d) a helytelen alkalmazási gyakorlat megszüntetése mellett indokolt esetben a személyi felelősség megállapításra kerüljön, a szükséges intézkedések megvalósuljanak.

Minden szervezeti egység vezetője felelős a feladatkörébe tartozó szakterületen észlelt adatvédelmet sértő esemény ismételt előfordulásának megelőzéséhez szükséges intézkedések megtételéért, a bekövetkezett esemény feltárásáért, szükség esetén annak dokumentálásáért, továbbá indokolt esetben a felelősségre vonással és a hiányosságok megszüntetésével kapcsolatos intézkedések kezdeményezéséért és megvalósításuk ellenőrzéséért.

A munkavállalók konkrét feladatát, hatáskörét, felelősségét a munkaköri leírások tartalmazzák. Valamennyi munkavállaló feladata és kötelessége az észlelt adatvédelmet sértő esemény jelzése az adott szervezeti egység vezetője felé a hierarchia betartásával és megszüntetésük érdekében javaslatok tétele, valamint az elrendelt intézkedések megvalósítása.

4. Az adatvédelmet sértő esemény észlelése, feltárása, bejelentése

Az adatvédelmet sértő esemény észlelése az ÁKK Zrt. munkatársai, vezetői, az ellenőrzést végző belső és külső szervek, vagy harmadik személy részéről történhet.

4.1. Az ÁKK Zrt. munkatársa által észlelt adatvédelmet sértő esemény esetén:

Amennyiben az adatvédelmet sértő eseményt munkatárs észleli, soron kívül köteles értesíteni – a hivatali út betartásával – az adatvédelemért felelős személyt és a közvetlenül felette álló vezetőt.

Amennyiben a munkatárs úgy ítéli meg, hogy közvetlen felettese az adott ügyben érintett, akkor a vezető felettesét kell értesítenie.

A munkatárs által a vezetőnek jelzett, vagy a vezető által észlelt adatvédelmet sértő esemény esetén amennyiben az lehetséges, saját hatáskörben kell az adatvédelmet sértő esemény megszüntetése érdekében a szükséges intézkedést meghozni.

Az adatvédelmi incidens bejelentése a felügyeleti hatóságnak:

Az adatvédelmi incidenst, indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens az adatvédelemért felelő személy tudomására jutott, bejelenteni köteles az illetékes felügyeleti hatóságnál, kivéve, ha az elszámoltathatóság elvével összhangban az ÁKK Zrt. bizonyítani tudja, hogy az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Ha a bejelentés 72 órán belül nem tehető meg, abban meg kell jelölni a késedelem okát, az előírt információkat pedig – további indokolatlan késedelem nélkül – részletekben is közölni lehet.
Az adatfeldolgozó az adatvédelmi incidenst, az arról való tudomásszerzését követően indokolatlan késedelem nélkül bejelenti az ÁKK Zrt.-nek.

A felügyeleti hatóság részére történő bejelentésben legalább:
- ismertetni kell az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát;
- közölni kell az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;
- ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket;
- ismertetni kell az ÁKK Zrt., mint adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

Amennyiben nem lehetséges az információkat egyidejűleg közölni, azok további indokolatlan késedelem nélkül később részletekben is közölhetők.
Az ÁKK Zrt., mint adatkezelő nyilvántartja az adatvédelmi incidenseket, feltüntetve az adatvédelmi incidenshez kapcsolódó tényeket, annak hatásait és az orvoslására tett intézkedéseket. E nyilvántartás lehetővé teszi, hogy a felügyeleti hatóság ellenőrizze a GDPR követelményeinek való megfelelést.

Az érintettet az ÁKK Zrt. indokolatlan késedelem nélkül tájékoztatja, ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, annak érdekében, hogy megtehesse a szükséges óvintézkedéseket. Az tájékoztatásnak tartalmaznia kell annak leírását, hogy milyen jellegű az adatvédelmi incidens, valamint az érintett a természetes személynek szóló, a lehetséges hátrányos hatások enyhítését célzó javaslatokat. Az érintettek tájékoztatásáról az észszerűség[11] keretei között a lehető leghamarabb gondoskodni kell, szorosan együttműködve a felügyeleti hatósággal, és betartva az általa vagy más érintett hatóságok (például bűnüldöző hatóságok) által adott útmutatást.

Késedelem nélkül meg kell bizonyosodni arról, hogy az összes megfelelő technológiai védelmi és szervezési intézkedés végrehajtásra került-e, egyrészt az adatvédelmi incidens haladéktalan

[11] Például az érintettek sürgős tájékoztatása a kár közvetlen veszélyének mérsékléséhez szükséges, azonban annak megelőzése több időt igényelhet, hogy a folyamatos vagy azonos jellegű adatvédelmi incidens esetében megfelelő intézkedéseket kell végrehajtani.

megállapítása, másrészt a felügyeleti hatóságnak történő bejelentés és az érintett sürgős értesítése érdekében. Azt, hogy az értesítésre indokolatlan késedelem nélkül került-e sor, különösen az adatvédelmi incidens jellegére és súlyosságára, valamint annak az érintettre gyakorolt következményeire, illetve hátrányos hatásaira figyelemmel kell megállapítani. A felügyeleti hatóságnak történt bejelentést a GDPR-ban meghatározott feladataival és hatásköreivel összhangban történő beavatkozását eredményezheti.

Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az ÁKK Zrt. indokolatlan késedelem nélkül tájékoztatja az érintettet az adatvédelmi incidensről.

Az érintett részére adott tájékoztatásban világosan és közérthetően ismertetni kell az adatvédelmi incidens jellegét, és közölni kell legalább a GDPR 33. cikk (3) bekezdésének b), c) és d) pontjában említett információkat és intézkedéseket.[12]

Az érintettet nem kell tájékoztatni, ha a következő feltételek bármelyike teljesül:
- az ÁKK Zrt. megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre, és ezeket az intézkedéseket az adatvédelmi incidens által érintett adatok tekintetében alkalmazták, különösen azokat az intézkedéseket – mint például a titkosítás alkalmazása –, amelyek a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik az adatokat;
- az ÁKK Zrt. az adatvédelmi incidenst követően olyan további intézkedéseket tett, amelyek biztosítják, hogy az érintett jogaira és szabadságaira jelentett, a magas kockázat a továbbiakban valószínűsíthetően nem valósul meg;
- a tájékoztatás aránytalan erőfeszítést tenne szükségessé.

Ilyen esetekben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, vagy olyan hasonló intézkedést kell hozni, amely biztosítja az érintettek hasonlóan hatékony tájékoztatását.

A bejelentő védelme
Amennyiben a bejelentő nevének elhallgatását kéri, úgy az eljárás folyamatában biztosítani kell adatainak a zárt kezelését, amelyet csak jogköre alapján az adatvédelemért felelős személy ismerhet meg.

A bejelentést tevő személlyel szemben nem alkalmazható semmiféle hátrányos elbánás, jelentéséért – kivéve a szándékosan valótlan tartalommal megtett jelentést – felelősségre nem vonható.

4.2. Külső ellenőrzési szerv által észlelt szabálytalanság

A felügyeleti hatóság által végzett ellenőrzés szabálytalanságra vonatkozó megállapításait az általa készített dokumentáció tartalmazza.

[12] GDPR 33. cikk (3) bekezdése:
(3) Az (1) bekezdésben említett bejelentésben legalább:
a) ismertetni kell az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát;
b) közölni kell az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;
c) ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket;
d) ismertetni kell az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

4.3. Külső személy által észlelt adatvédelmet sértő esemény

Amennyiben külső személy jelzi az adatvédelmet sértő eseményt, az érintett szervezeti egység vezetőjének a bejelentést érdemben kell megvizsgálnia és jegyzőkönyvet felvennie a bejelentés beérkezését követő 3 munkanapon belül.

Ha nem az érintett szervezeti egységhez érkezett a jelzés, azt az érkezést követő legfeljebb 3 munkanapon belül továbbítani kell az érintett szervezeti egység részére.

5. Az adatvédelmet sértő esemény megszüntetésére tett intézkedések

5.1 A szabálytalanság megszüntetése esetén követendő eljárás

A munkatárs által önellenőrzéssel észlelt, illetőleg a belső kontrollrendszer keretében az előzetes, utólagos és vezetői ellenőrzés során kiszűrt, a hatáskörrel rendelkező szervezeti egység vezetője által elrendelt javítással, helyesbítéssel megszüntethető hiba korrigálása nem igényel szabálytalansági eljárást.

A felderítés során az alábbi kategóriák valamelyikébe kell az adatvédelmi incidenst sorolni:

- *Alacsony szintű adatvédelmi incidens:* a személyes adatok elhanyagolható körének jogosulatlan továbbítása, megváltoztatása, nyilvánosságra hozatala, szándékolt, vagy véletlen törlése vagy megsemmisítése, vagy más jogellenes adatkezelési eset.
- *Közepes szintű adatvédelmi incidens:* a személyes adatok csekély körének megváltoztatása, jogosulatlan továbbítása, nyilvánosságra hozatala, szándékolt, vagy véletlen törlése vagy megsemmisítése, vagy más jogellenes adatkezelési eset.
- *Magas szintű adatvédelmi incidens:*
    - a személyes adatok széles körének jogosulatlan megváltoztatása, továbbítása, nyilvánosságra hozatala, szándékolt, vagy véletlen törlése vagy megsemmisítése, vagy más jogellenes adatkezelési eset, illetve
    - az adatok körétől függetlenül minden olyan eset, amikor valószínűsíthető vagy biztosra vehető, hogy az incidensnek az érintettre hátrányos hatása van.

A szabálytalanság megszüntetésére a hatáskörrel rendelkező vezetőnek, az informatikai biztonsági munkatársnak, az érintett szervezeti egység vezetőjének, illetve ha indokolt az ÁKK Zrt. vezérigazgatójának kell intézkednie.
A szabálytalanság kivizsgálásában nem vehet részt, aki elfogult, akitől az ügy tárgyilagos megítélése nem várható el.

5.2 Az adatvédelmet sértő esemény megszüntetése

5.2.1. Az eljárás során a következő teendőket kell végrehajtani:

a) Összegyűjteni az adatokat, információkat;
b) Értékelni az adatokat, információkat;
c) Megoldási javaslatot készíteni a nemkívánatos helyzet kezelésére (intézkedési terv készítése – feladat, felelős, határidő megjelöléssel);
d) Dokumentálni az eljárást;
e) Jóváhagyásra elkészíteni a javasolt intézkedési tervet;
f) Az adatvédelemért felelős személynek nyomon követni a jóváhagyott intézkedési terv megvalósulását, amennyiben az szükséges, egyeztetéseket, megbeszéléseket összehívni;
g) Az adatvédelemért felelős személynek a folyamatban érintettek részére tájékoztatást nyújtani a feladatok előrehaladásáról, az adatvédelmet sértő esemény kezeléséről.

Alacsony szintű adatvédelmi incidens esetén az adatvédelemért felelős személy, illetve az adatvédelmi tisztviselő és az informatikai biztonsági munkatárs:

- legkésőbb a tudomásszerzéstől számított 2 munkanapon belül az érintett rendszer üzemeltetéséért felelős vezetőjével és az adatvédelmi incidenssel érintett adatkezelési folyamat adatgazdájával meghatározza az adatvédelmi incidens kezelésének módját és felhívja az intézkedésre jogosult személyt az incidens kezelésére,
- rögzíti az adatvédelmi incidenst az incidensek nyilvántartásába.

Közepes szintű adatvédelmi incidens esetén:

- haladéktalanul, de legkésőbb a tudomásszerzést követő munkanapon munkacsoportot hív össze, amelyben részt vesz az adatvédelemért felelős személy (adatvédelmi tisztviselő) és informatikai biztonsági munkatárson kívül a szakterület vezetője, az adatvédelmi incidenssel érintett adatkezelési folyamat adatgazdája és az ÁKK Zrt. vezérigazgatója,
- a munkacsoport meghatározza az adatvédelmi incidens kezelésének módját és felhívja az intézkedésre jogosult személyt az incidens kezelésére,
- az adatvédelemért felelős személy rögzíti az adatvédelmi incidenst az incidensek nyilvántartásában,
- az adatvédelemért felelős személy (adatvédelmi tisztviselő) értesíti a felügyeleti hatóságot 72 órán belül az adatvédelmi incidensről, ha az adatvédelmi incidens valószínűsíthetően kockázattal jár az érintett vagy más érintettek jogaira és szabadságaira nézve.

Magas szintű adatvédelmi incidens esetén

- haladéktalanul, de legkésőbb a tudomásszerzéstől számított 24 órán belül munkacsoportot hív össze, amelyben részt vesz az adatvédelemért felelős személyen kívül a szakterület vezetője, az adatvédelmi incidenssel érintett adatkezelési folyamat adatgazdája és az ÁKK Zrt. vezérigazgatója,
- a munkacsoport meghatározza az adatvédelmi incidens kezelésének módját és felhívja az intézkedésre jogosult személyt az incidens kezelésére, továbbá meghatározza az érintettek értesítésének módját, az értesítés tartalmát, és gondoskodik az érintettek haladéktalan értesítéséről
- az adatvédelemért felelős személy (adatvédelemi tisztviselő) rögzíti az adatvédelmi incidenst az incidensek nyilvántartásában,
- az adatvédelemi tisztviselő értesíti a felügyeleti hatóságot a tudomásszerzéstől számított 72 órán belül az adatvédelmi incidensről.

5.2.2. Az adatvédelmet sértő eseményt vizsgáló eljárás eredménye, intézkedési javaslat

Az eljárás eredménye lehet:

a) annak megállapítása, hogy nem történt adatvédelmet sértő esemény és az eljárás intézkedés nélküli megszüntetése (pl. hibás észlelés);
b) adatvédelmet sértő esemény megtörténtét megállapító és intézkedést elrendelő döntés;
c) további eljárás elrendelése, amely a felelősség megállapítása vagy a hasonló esetek megelőzése érdekében szükséges.

5.2.3. Belső vagy külső ellenőrzés eredménye alapján szükséges intézkedés

A belső szakmai ellenőrzés, az adatvédelemért felelős személy által megállapított szabálytalanság, valamint az informatikai biztonságot fenyegető, vagy sértő esemény, cselekmény, illetve állapot, vagy az informatikai biztonsági szabályozások megszegését eredményező bármilyen cselekmény esetén a szabálytalansággal, nem megfelelőséggel, incidenssel érintett szervezeti egység vezetőjének a vonatkozó belső szabályzat előírása alapján intézkednie kell a megállapítások hatásos kezelésére.

A külső ellenőrzési szerv által megállapított szabálytalanság esetén az eljárási jelentésben foglalt szabálytalanságokra vonatkozó, az ellenőrzéssel érintett szakterület által kidolgozott intézkedési tervet végre kell hajtani.

6. Jogkövetkezmények alkalmazása

A jogkövetkezményekről való döntés kezdeményezése az adatvédelmet sértő esemény megszüntetésére a vezérigazgató, az érintett szervezeti egység vezető, a hatáskörrel rendelkező szervezeti egység vezető, illetve az adatvédelemért felelős személy feladata.

A jogkövetkezmény jellege szerint lehet:

a) jogi jellegű (kártérítési eljárás megindítása, szabálysértési vagy büntetőeljárás kezdeményezése az arra feljogosított hatóságnál),
b) munkajogi (figyelmeztetés, munkaviszony felmondással, azonnali hatállyal történő megszüntetése),
c) pénzügyi jellegű (pénzbeli juttatás, kifizetés részben vagy egészben történő felfüggesztése, visszakövetelése, behajtása),
d) szakmai jellegű (belső szabályozás módosítása, szigorításának kezdeményezése, betartásának fokozott ellenőrzése stb.).

Amennyiben büntető- vagy szabálysértési eljárás kezdeményezésének szükségessége merül fel, a szükséges intézkedések meghozatala az arra illetékes szervek értesítését is jelenti annak érdekében, hogy megalapozottság esetén az illetékes szerv a megfelelő eljárásokat megindítsa. Az eljárások megindításának kezdeményezésére a hatáskörrel rendelkező szervezeti egység vezetőjének javaslatára az ÁKK Zrt. vezérigazgatója jogosult.
Ha nyilvánvalóvá vált, hogy az adatvédelmet sértő eseményt bejelentő rosszhiszeműen járt el és alaposan feltehető, hogy ezzel bűncselekményt vagy szabálysértést követett el, másnak kárt vagy egyéb jogsérelmet okozott, adatai az eljárás kezdeményezésére, valamint lefolytatására jogosult részére átadhatók.

7. Az adatvédelmet sértő eseményekkel kapcsolatos intézkedések, eljárások nyomon követése

Az érintett szervezeti egységek vezetőinek feladata az adatvédelmet sértő eseményekkel kapcsolatos intézkedések, eljárások nyomon követése során:

a) az elrendelt eljárások, a meghozott döntések, illetve a megindított eljárások figyelemmel kísérése,
b) az eljárások során készített javaslatok, intézkedési tervek megvalósítása és a végrehajtás ellenőrzése,
c) a feltárt adatvédelmet sértő esemény alapján a további bekövetkezési lehetőségek beazonosítása, szükség esetén a belső szabályzatok, illetve jogszabályok módosításának kezdeményezése,
d) annak vizsgálata, hogy az ellenőrzési folyamatban rögzített eljárás az adott adatvédelmet sértő eseményt miért nem szűrte ki, indokolt esetben gondoskodni kell az ellenőrzési folyamat felülvizsgálatáról, helyesbítéséről.

Amennyiben az intézkedések végrehajtása során megállapítást nyer, hogy az alkalmazott intézkedések nem elég hatásosak, a hatáskörrel rendelkező szervezeti egység vezetője további intézkedést rendel el.

5. számú melléklet – Vonatkozó jogszabályok

Ezen szabályzat különösen az alábbi jogszabályok rendelkezéseinek figyelembevételével készült:

1. Magyarország Alaptörvénye,
2. 2013. évi V. törvény a Polgári Törvénykönyvről,
3. 2011. évi CXCV. törvény az államháztartásról,
4. 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról,
5. 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 szóló Európai Parlament és a Tanács (EU) 2016/679 rendelete
6. 2012. évi I. törvény a Munka törvénykönyvéről,
7. 2009. évi CLV. törvény a minősített adatvédelméről,
8. 2007. évi CXXXVIII. törvény a befektetési vállalkozásokról és az árutőzsdei szolgáltatókról, valamint az általuk végezhető tevékenységek szabályairól,
9. 2013. évi CCXXXVII. törvény a hitelintézetekről és a pénzügyi vállalkozásokról,
10. 1996. évi XX. törvény a személyazonosító jel helyére lépő azonosítási módokról és az azonosító kódok használatáról,
11. 2019. évi CXXII. törvény a társadalombiztosítás ellátásaira jogosultakról, valamint ezen ellátások fedezetéről ,
12. 2006. évi V. törvény a cégnyilvántartásról, a cégnyilvánosságról és a bírósági cégeljárásról,
13. 2000. évi C. törvény a számvitelről,
14. 2001. évi CXX. törvény a tőkepiacról,
15. 2017. évi LIII. törvény a pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról,
16. 2017. évi CL. törvény az adózás rendjéről,
17. 2015. évi CXLIII. törvény a közbeszerzésekről,
18. 1995. évi CXVII. törvény a személyi jövedelemadóról.
19. 2018. évi LIV. törvény az üzleti titok védelméről
20. 301/2016 (IX.30.) Korm. rendelet