ADATVÉDELMI ÉS ADATBIZTONSÁGI SZABÁLYZAT

KÍSÉRLETI ORVOSTUDOMÁNYI KUTATÓINTÉZET

Tartalom

1. A szabályzat célja és hatálya

A Kísérleti Orvostudományi Kutatóintézet (a továbbiakban: „KOKI") az adatkezelés jogszerűségének biztosítása érdekében Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) 25/A. § (3) bekezdésében foglalt kötelezettségének eleget téve elkészítette a jelen adatvédelmi és adatbiztonsági szabályzatát (a továbbiakban: „Szabályzat"), melynek célja, biztosítsa a KOKI által kezelt adatok vonatkozásában az adatvédelem alkotmányos elveinek, az adatbiztonság követelményeinek érvényesülését, megakadályozza a jogosulatlan hozzáférést, az adatok megváltoztatását és jogosulatlan nyilvánosságra hozatalát, valamint meghatározza a KOKI által vezetett, adatvédelemmel kapcsolatos nyilvántartások kezelésének rendjét.

Jelen Szabályzat hatálya kiterjed a KOKI minden szervezeti egységére, munkavállalójára és a KOKI megbízásából az adatkezelésbe bekapcsolódó szervezetekre és személyekre.
Kiterjed továbbá azon személyekre, akik adatait a jelen Szabályzat hatálya alá tartozó adatkezelések tartalmazzák és azokra, akiknek jogait vagy jogos érdekeit az adatkezelés érinti.

2. A szabályzatot az alábbi jogszabályokkal összehangban kell alkalmazni:

- GDPR (Adatvédelmi Rendelet) - AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről);
- Adatvédelmi törvény - Az információs önrendelkezési jogról, és az információszabadságról szóló 2011. évi CXII. törvény és a végrehajtására kiadott jogszabályok;
- A Polgári Törvénykönyvről szóló 2013. évi V. törvény;
- Az adózás rendjéről szóló 2017. évi CL. törvény és végrehajtására kiadott jogszabályok;
- A számvitelről szóló 2000. évi C. törvény és végrehajtására kiadott jogszabályok;
- Mt. - A munka törvénykönyvéről szóló 2012. évi I. törvény.

3. A szabályzatot az alábbi belső szabályzatokkal összehangban kell alkalmazni:

- Kamerarendszer Üzemeltetési Szabályzat
- Iratkezelési Szabályzat
- Incidenskezelési Terv
- Szabályzat a közérdekű adatok megismerésére irányuló igények teljesítésének rendjéről
- Szabályzat a közérdekű és közérdekből nyilvános adatok elektronikus közzétételének rendjéről
- Adatkezelések nyilvántartása

- Az együttműködő cégek nyilvántartása
- Adatvédelmi incidensek nyilvántartása

4. Fogalommeghatározások

személyes adat	A természetes személyre (érintettre) vonatkozó bármely információ (pl.: név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó adat)
különleges adat	Ilyenek 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.
egészségügyi adat	Egy természetes személy testi vagy pszichikai egészségi állapotára vonatkozó személyes adat, ideértve a természetes személy számára nyújtott egészségügyi szolgáltatásokra vonatkozó olyan adatot is, amely információt hordoz a természetes személy egészségi állapotáról.
érintett	Az azonosítható természetes személy, akire az adott személyes adat vonatkozik. Az Ön személyes adatai tekintetében Ön az érintett.
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.
adatfeldolgozás	Az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése.
adatfeldolgozó	Az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az Munkáltató nevében (megbízásából, utasítására és a Munkáltató döntése alapján) személyes adatokat kezel.
profilalkotás	Személyes adatok automatizált kezelésének bármely olyan formája, amelynek során a személyes adatokat valamely természetes személyhez fűződő bizonyos személyes jellemzők értékelésére, különösen a munkahelyi teljesítményhez, gazdasági helyzethez, egészségi állapothoz, személyes preferenciákhoz, érdeklődéshez, megbízhatósághoz, viselkedéshez, tartózkodási helyhez vagy

	mozgáshoz kapcsolódó jellemzők elemzésére vagy előrejelzésére használják.
harmadik fél	Az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely nem azonos az érintettel, az Munkáltatóval, az adatfeldolgozóval vagy azokkal a személyekkel, akik az Munkáltató vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére felhatalmazást kaptak.
az érintett hozzájárulása	Az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez;
adatvédelmi Tisztviselő	A KOKI által megbízott Tisztviselő, aki támogatást nyújt a megfelelő adatkezelési gyakorlat megvalósításában és működtetésében, szükség esetén kapcsolatot tart a felügyeleti hatósággal és az érintettekkel.
az adatkezelés korlátozása	A tárolt személyes adatok megjelölése jövőbeli kezelésük korlátozása céljából.
álnevesítés	A személyes adatok olyan módon történő kezelése, amelynek következtében további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik, feltéve, hogy az ilyen további információt külön tárolják, és technikai és szervezési intézkedések megtételével biztosított, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet kapcsolni.
nyilvántartási rendszer	A személyes adatok bármely módon – centralizált, decentralizált vagy funkcionális vagy földrajzi szempontok szerint – tagolt állománya, amely meghatározott ismérvek alapján hozzáférhető.
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.
harmadik fél	Az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely nem azonos az érintettel, az adatkezelővel, az adatfeldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére felhatalmazást kaptak.
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.

5. Adatvédelmi alapelvek

5.1. Jogszerűség, tisztességes eljárás és átláthatóság elve

A személyes adatok kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni.

5.2. Célhoz kötöttség elve

A személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történjen, és azokat ne kezeljék ezekkel 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.

5.3. Adattakarékosság elve

A személyes adatok az adatkezelés céljai szempontjából megfelelőek és relevánsak kell, hogy legyenek, és a szükségesre kell korlátozódniuk.

5.4. Pontosság elve

A személyes adatok pontosnak és szükség esetén naprakésznek kell lenniük; minden észszerű intézkedést meg kell tenni annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul töröljék vagy helyesbítsék.

5.5. Korlátozott tárolhatóság elve

A személyes adatok tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi 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, az e rendeletben az érintettek jogainak és szabadságainak védelme érdekében előírt megfelelő technikai és szervezési intézkedések végrehajtására is figyelemmel.

5.6. Integritás és bizalmas jelleg

A személyes adatok kezelését oly módon kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve.

5.7. Elszámoltathatóság elve

Az adatkezelő felelős az alapelveknek való megfelelésért, továbbá képesnek kell lennie e megfelelés igazolására.

6. Az érintettek jogai és érvényesítésük

6.1. Hozzájárulás visszavonása

Kizárólag az érintett hozzájárulása alapján végzett adatkezelések esetén, az érintett bármikor visszavonhatja a hozzájárulását. Ilyen esetben az erről szóló értesítést követően – amennyiben más jogalapon nem történik adatkezelés – törölni kell az érintett személyes adatait. Erről, valamint arról, hogy a visszavonás előtt a hozzájárulás alapján végzett adatkezelés jogszerűségét nem érinti, az érintettet tájékoztatni kell.

6.2. Tájékoztatás (hozzáférést) kérése

A GDPR két külön listában sorolja fel – GDPR 13. és 14. cikk - azt, hogy pontosan miről kell tájékoztatni az érintettet, attól függően, hogy az adatok az érintettől közvetlenül, vagy valaki mástól származnak.

A tájékoztatás legegyszerűbben egy általános tájékoztatóval végezhető el *(Adatkezelési Tájékoztató, Munkavállalók Adatkezelési Tájékoztatója, Kamerarendszerről szóló Tájékoztató, stb)*. Lehetnek azonban olyan esetek, amikor esetileg kell tájékoztatni az érintettet. A félreértések elkerülése, és pontos tájékoztatás érdekében törekedni kell az írásos tájékoztatásra, valamint kérni meg az érintettet, hogy szóban feltett kérdéseit - amennyiben arra az általános tájékoztatókban nem talál választ – írásban, az adatvedelem@koki.hu e-mailcímre küldje meg.

Az érintett tájékoztatást kérhet arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e, és ha igen:

- Mi a célja?
- Pontosan milyen adatok kezeléséről van szó?
- Kinek kerülnek továbbításra ezek az adatok?
- Meddig történik a tárolása ezeknek az adatoknak?
- Az érintettnek milyen jogai és jogorvoslati eszközei vannak ezzel kapcsolatban?
- Kitől kaptuk az érintett adatait?
- Van-e automatizált döntés az érintettre vonatkozóan (ideértve a profilalkotást is) az érintett személyes adatai felhasználásával? Ilyen esetekben arról is kérhető tájékoztatást, hogy milyen logikát (módszert) alkalmaz a KOKI, és arról, hogy az ilyen adatkezelés milyen jelentőséggel bír, milyen várható következményekkel jár.
- Ha az érintett azt tapasztalta, hogy adatait nemzetközi szervezet, vagy harmadik ország (nem uniós tagállam) felé továbbításra került, úgy kérheti annak bemutatást, hogy mi garantálja személyes adatai megfelelő kezelését.
- Kérhet másolatot a kezelt személyes adatairól (A további másolatokért az adminisztratív költségeken alapuló díjat számítható fel.)

6.3. Helyesbítés kérése

Az érintett kérheti a pontatlanul, vagy hiányosan rögzített személyes adata javítását vagy kiegészítését. Ilyen kérés esetén a javítást vagy kiegészítést haladéktalanul el kell végezni, és

erről az érintettet tájékoztatni kell. Ha az adatot másnak is továbbításra került, értesíteni kell a továbbítás címzettjét is.

6.4. Törléshez való jog („elfeledtetés joga”)

Az érintett kérheti a személyes adatai törlését:

- ha a személyes adatokra már nincs szükség abból a célból, amelyből azok kezelése történt;
- pusztán az érintett hozzájárulása alapján végzett adatkezelések esetén;
- ha megállapításra kerül, hogy a személyes adatokat kezelése jogellenes, a tiltakozás eredményes;
- ha Uniós vagy hazai jogszabály előírja;
- ha a személyes adatokat uniós vagy tagállami jogban előírt jogi kötelezettség teljesítéséhez törölni kell;
- ha a személyes adatok gyűjtésére az információs társadalommal összefüggő, gyermekek részére kínált szolgáltatásokkal kapcsolatosan került sor.

Ha a személyes adatok nyilvánosságra hozatala megtörtént, és azt a fentiek értelmében törölni kell, az elérhető technológia és a megvalósítás költségeinek figyelembevételével meg kell tenni az észszerűen elvárható lépéseket – ideértve technikai intézkedéseket –az adatokat kezelő adatkezelők tájékoztatása érdekében, hogy az érintett kérelmezte a szóban forgó személyes adatokra mutató linkek vagy e személyes adatok másolatának, illetve másodpéldányának törlését.

A személyes adatokat nem törölhetők, amennyiben azokra szükség van:

- a véleménynyilvánítás szabadságához és a tájékozódáshoz való jog gyakorlása céljából;
- a személyes adatok kezelését előíró, az adatkezelőre alkalmazandó uniós vagy tagállami jog szerinti kötelezettség teljesítése, illetve közérdekből;
- a népegészségügy területét érintő közérdek alapján;
- közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból, amennyiben a törlés valószínűsíthetően lehetetlenné tenné vagy komolyan veszélyeztetné ezt az adatkezelést; vagy
- jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez.

A törlés kérésénél a nagy körültekintéssel kell eljárni a tekintetben, hogy az adat valóban törölhető-e. A törlésről tájékoztatni kell az érintettet és azt, aki felé adattovábbítás történt. Amennyiben bármilyen okból nem, vagy nem teljesen tudjuk törölni az adatokat, az érintettet értesíteni szükséges, és egyeztetni a mindenki számára megfelelő megoldás megtalálása érdekében.

6.5. Kérés az adatkezelés korlátozása iránt

Az érintett kérheti, hogy az adatkezelés korlátozását, ha az alábbiak valamelyike teljesül:

- az érintett vitatja a személyes adatok pontosságát, ez esetben a korlátozás arra az időtartamra vonatkozik, amely lehetővé teszi a személyes adatok pontosságának ellenőrzését;
- az adatkezelés jogellenes, de az érintett ellenzi az adatok törlését, és ehelyett kéri azok felhasználásának korlátozását;
- már nincs szükség a személyes adatokra az adatkezelés céljából, de az érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez;
- az érintett tiltakozott az adatkezelés ellen; ez esetben a korlátozás arra az időtartamra vonatkozik, amíg megállapításra nem kerül, hogy az Adatkezelő jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben.

Korlátozás esetén a 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 Unió, illetve valamely tagállam fontos közérdekéből lehet kezelni.

A korlátozás esetleges feloldásáról előzetesen tájékoztatni kell az érintettet.

6.6. Adathordozhatósághoz való jog

Kizárólag hozzájárulás, vagy szerződéses jogalapon automatizált módon végzett adatkezelések estén az érintett jogosult arra, hogy személyes adatait géppel olvasható formátumban megkapja.

6.7. Tiltakozás

Az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból bármikor tiltakozzon személyes adatainak kezelése ellen, ha a közérdekű feladat végrehajtásához szükséges.

Ebben az esetben az adatkezelő a személyes adatokat nem kezelheti tovább, kivéve, ha az adatkezelő bizonyítja, hogy az adatkezelést olyan kényszerítő erejű jogos okok indokolják, amelyek elsőbbséget élveznek az érintett érdekeivel, jogaival és szabadságaival szemben, vagy amelyek jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódnak. Az említett jogra legkésőbb az érintettel való első kapcsolatfelvétel során kifejezetten fel kell hívni annak figyelmét, és az erre vonatkozó tájékoztatást egyértelműen és minden más információtól elkülönítve kell megjeleníteni.

Az érintett akkor is tiltakozhat a személyes adatai kezelése ellen, ha: a személyes adatok kezelésére tudományos és történelmi kutatási célból vagy statisztikai célból kerül sor. Ebben az esetben a személyes adatokat mérlegelés nélkül törölni kell.

6.8. Érintetti igények teljesítése

A fent részletezett jogok illetik meg, melyekkel kapcsolatban szóban, postai vagy bármilyen elektronikus úton (e-mail, telefon, fax) fordulhatnak a KOKI-hoz.

Azonosítás
A kérés teljesítése előtt minden esetben azonosítani kell az érintett személyazonosságát. Ha az azonosítás nem lehetséges, a kérés nem teljesíthető.

A kérés megválaszolása
Az azonosítást követően írásban, elektronikusan, vagy - az érintett kérésére - szóban kell tájékoztatást nyújtani a kéréssel kapcsolatban. Ha az érintett elektronikus úton nyújtotta be a kérelmet, elektronikus úton kell válaszolni. Természetesen ebben az esetben is van lehetősége más módot kérni.

Ügyintézési határidő
Legkésőbb a kérés beérkezésétől számított 1 (Egy) hónapon belül tájékoztatni kell az érintettet a kérése nyomán hozott intézkedésekről. Szükség esetén, figyelembe véve a kérelem összetettségét és a kérelmek számát, ez a határidő további 2 (Kettő) hónappal meghosszabbítható, amiről még az egy hónapos ügyintézési határidőn belül tájékoztatni kell az érintettet.

Az intézkedés elmaradásáról is tájékoztatni kell az érintettet az egy hónapos ügyintézési határidőn belül. Ez ellen panaszt nyújtható be a NAIH-nál, és az érintett élhet bírósági jogorvoslati jogával.

Az ügyintézés díja
A kért tájékoztatás és intézkedés díjmentes. Kivételt képez az eset, ha a kérés egyértelműen megalapozatlan vagy – különösen ismétlődő jellege miatt – túlzó. Ebben az esetben díj számolható fel, vagy megtagadható a kérés teljesítése.

7. A KOKI adatvédelmi szervezete

7.1. A KOKI igazgatója

Az adatvédelmi előírások alkalmazása során az adatkezelő/adatfeldolgozó szerv vezetőjének a KOKI igazgatója minősül.

A KOKI igazgatója határozatlan időre az adatvédelmi jogot és gyakorlatot szakértői szinten ismerő adatvédelmi tisztviselőt nevez ki.

7.2. Adatvédelmi tisztviselő

A GDPR 37. cikke alapján az adatkezelő adatvédelmi tisztviselőt köteles kijelölni minden olyan esetben, amikor az adatkezelést közfeladatot ellátó szerv végzi. A KOKI esetén tehát kötelező az adatvédelmi tisztviselő kinevezése.

Az adatvédelmi tisztviselő az alábbi feladatok ellátására köteles:

- Tájékoztat és szakmai tanácsot ad az adatkezelő vagy az adatfeldolgozó, továbbá az adatkezelést végző alkalmazottak részére az e rendelet, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezések szerinti kötelezettségeikkel kapcsolatban;
- Ellenőrzi az e rendeletnek, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezéseknek, továbbá az adatkezelő vagy az adatfeldolgozó személyes adatok védelmével kapcsolatos belső szabályainak való megfelelést, ideértve a feladatkörök

kijelölését, az adatkezelési műveletekben részt vevő személyzet tudatosság-növelését és képzését, valamint a kapcsolódó auditokat is;
- Kérésre szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, valamint nyomon követi a hatásvizsgálat GDPR. 35. cikk szerinti elvégzését;
- Együttműködik a felügyeleti hatósággal;
- Az adatkezeléssel összefüggő ügyekben – ideértve a GDPR 36. cikkben említett előzetes konzultációt is – kapcsolattartó pontként szolgál a felügyeleti hatóság felé, valamint adott esetben bármely egyéb kérdésben konzultációt folytat vele.

Az adatvédelmi tisztviselő feladatkörei bővíthetők.

Az adatvédelmi tisztviselőt szakmai rátermettség és különösen az adatvédelmi jog és gyakorlat szakértői szintű ismerete, valamint a GDPR. 39. cikkben említett feladatok ellátására való alkalmasság alapján kell kijelölni.

Releváns készségek és szakértelem például:

- szakértelem a nemzeti és európai adatvédelmi jogszabályok és gyakorlatok terén, beleértve a GDPR alapos ismeretét;
- az elvégzett adatkezelési műveletek ismerete;
- az információs technológiák és az adatbiztonság ismerete;
- az üzletág és a szervezet ismerete;
- a szervezeten belül az adatvédelmi kultúra előmozdításának képessége.

Az adatvédelmi tisztviselő az adatkezelő vagy az adatfeldolgozó alkalmazottja lehet, vagy szolgáltatási szerződés keretében láthatja el a feladatait. Bár az adatvédelmi tisztviselőknek lehet más feladatuk, csak olyan egyéb feladatokkal bízhatók meg, amelyek nem okoznak összeférhetetlenséget. A GDPR 38. cikk (3) bekezdése szerint az adatvédelmi tisztviselőt úgy kell kijelölni, hogy senkitől ne fogadhasson el utasításokat a tisztviselői feladatának ellátásával kapcsolatban. Az adatvédelmi tisztviselő közvetlenül az adatkezelő legfelső vezetésének tartozik felelősséggel. Ugyanakkor az adatvédelmi tisztviselő nem tölthet be olyan pozíciót a szervezeten belül, amelynek keretében ő határozza meg a személyes adatok kezelésének céljait és eszközeit, vagyis nem lehet vezető sem.

Az adatvédelmi tisztviselő elérhetőségét közzé kell tenni és a személyét a NAIH felé be kell jelenteni az erre kialakított online felületen.

7.3. Szervezeti egységek vezetői

Felelősek azért, hogy az irányításuk vagy vezetésük alatt álló szervezeti egységeknél az adatkezelés a jogszabályokban és a Szabályzatban meghatározottak szerint történjen.

7.4. Adatkezelést végző munkatársak

- kezelik és megőrzik a feladat-, illetve a munkakörük ellátása során birtokukba került adatokat;
- betartják az adatkezelésre vonatkozó jogszabályokat és belső irányítási eszközöket

- kötelesek a Társaságnál szervezett adatvédelmi oktatásokon részt venni;
- az adatkezeléssel kapcsolatosan feltárt szabálytalanságokat kötelesek haladéktalanul megszüntetni, mely érdekében az adatvédelmi tisztviselővel egyeztetnek.

8. A munkavállalók személyes adatainak kezelése

A KOKI a munkatársainak személyes adatait a munkaviszony, munkavégzésre irányuló egyéb jogviszony létesítésével, fennállásával és megszüntetésével, valamint az abból származó jogok gyakorlásával és kötelezettségek teljesítésével összefüggésben kezelheti.

8.1. A munkavállalók tájékoztatása az adatkezelésről

A munkába lepés előtt, de legkésőbb a munkába lépés napján a munkavállalók részére át kell adni a Munkavállalók Adatkezelési Tájékoztatóját és a Tájékoztatót Kamerarendszer és a Tájékoztatót Beléptető rendszer üzemeltetéséről. A tájékoztatók átvételét a munkavállaló aláírásával igazolja. Az átvétel igazolását a munkavállaló személyi anyagában a munkavállaló kilépéséig meg kell őrizni.

Ha a munkavállalók nagy száma miatt a tájékoztatók fizikai átadására és átvételére nincsen mód, úgy megfelelő, a tájékoztatók elektronikus úton történő megküldése a munkavállaló részére. Ebben az esetben az átvételt az olvasási jelentés bizonyítja.

A tájékoztatók elérését a belső rendszerben szintén javasolt biztosítani.

Ha változik valamelyik tájékoztató, úgy a tájékoztató aktualizált példányát az eredeti példánnyal azonos módon kell a munkavállaló részére átadni.

Amennyiben a munkavállalónak kérdése van az adatkezeléssel kapcsolatban azt írásban jelezheti az adatvedelem@koki.hu e-mail címen.

8.2. Felelősség a munkavállalók adatainak kezeléséért

A munkaviszonnyal összefüggő adatok kezeléséért a KOKI-nál
- az igazgató,
- az érintett munkavállaló felettese,
- a személyzeti feladatot ellátó munkatárs,
- a munkavállaló - a saját adatainak közlése tekintetében - tartozik felelősséggel.

Az igazgató felel a munkaviszonnyal összefüggő adatok védelmére és kezelésére vonatkozó jogszabályok, valamint az e Szabályzatban rögzített előírások megtartásáért, illetve e követelmények teljesítésének ellenőrzéséért.

Az igazgató e felelősségi körében köteles gondoskodni:
- a Munkavállalók Adatkezelési Tájékoztatójának kiadásáról, kiegészítéséről, szükség esetén módosításáról,
- a munkaviszonnyal összefüggő adatok védelmével kapcsolatos követelmények

érvényesüléséről,
- a munkaviszonnyal összefüggő adatok kezelésére vonatkozó szabályok érvényesülésének folyamatos ellenőrzéséről,
- az ellenőrzés módszereinek és rendszerének kialakításáról és működtetéséről.

Az Igazgató szükség szerint átfogó, illetve eseti ellenőrzés keretében győződik meg a munkaviszonnyal összefüggő adatok védelmére és kezelésére vonatkozó jogszabályok megfelelő érvényesüléséről.

Az érintett munkavállaló felettese, kizárólag a számára nélkülözhetetlen személyes adatok megismerésére jogosult. Érintetti kérés esetén gondoskodik a kérés továbbításáról a személyzeti feladatokat ellátó munkatárs felé.

A személyzeti feladatot ellátó munkatárs felelősségi körén belül köteles gondoskodni arról, hogy:
- az általa kezelt személyes adat és megállapítás az adatkezelés teljes folyamatában megfeleljen a jogszabályi rendelkezések tartalmának,
- a személyi iratra csak olyan adat, illetve megállapítás kerülhessen, amely a jogszabályokban felsorolt adatforráson alapul, vagy egyéb okból igazolható módon feltétlenül szükséges;
- a munkaviszonnyal összefüggő adat helyesbítését és törlését kezdeményezze, ha megítélése szerint a személyi iraton szereplő adat a valóságnak már nem felel meg. Továbbá az ilyen irányú érintetti kérdések teljesítésében közreműködjön.

A **munkavállaló** felelős azért, hogy az általa átadott, bejelentett adatok hitelesek, pontosak, teljesek és aktuálisak legyenek.

8.3. Ellenőrzési jog

A munkavállaló a munkaviszonnyal összefüggő magatartása körében ellenőrizhető. Ennek keretében a munkáltató technikai eszközt is alkalmazhat, erről a munkavállalót előzetesen írásban tájékoztatja. A munkavállaló a munkáltató által a munkavégzéshez biztosított információtechnológiai vagy számítástechnikai eszközt, rendszert - eltérő megállapodás hiányában - kizárólag a munkaviszony teljesítése érdekében használhatja.

A munkáltató ellenőrzése során a munkaviszony teljesítéséhez használt számítástechnikai eszközön tárolt, a munkaviszonnyal összefüggő adatokba tekinthet be. Az ellenőrzési jogosultság szempontjából munkaviszonnyal összefüggő adatnak minősül a korlátozás betartásának ellenőrzéséhez szükséges adat. Ezt akkor is alkalmazni kell, ha a felek megállapodása alapján a munkavállaló a munkaviszony teljesítése érdekében saját számítástechnikai eszközt használ.

8.4. Munkavállalók adatvédelmi oktatása

KOKI az adatvédelmi tisztégviselő és az Igazgató közreműködésével évente adatvédelmi oktatást szervez annak érdekében, hogy a munkatársak megismerjék az általuk alkalmazandó adatvédelmi előírásokat és megfelelően járjanak el azok alkalmazása során.

9. Az álláskeresők személyes adatainak kezelése

Álláspályázat kiírása során tájékoztatást kell nyújtani a leendő jelentkezők részére a kiválasztást befolyásoló kritériumokról és a lehetséges háttérkutatásokról is. Így például ismertetni kell a jelentkezőkkel, hogy a felvételi eljárás folyamata kiterjed arra is, hogy a leendő munkáltató megtekinti a jelentkező közösségi oldalon létrehozott, bárki számára nyilvános információit. A jelentkező közösségi oldalon végzett, nyilvános tevékenysége megismerhető, arról következtetés levonható, de a további adatkezelési műveletek már jogellenesnek minősülnek. Vagyis arra nincs lehetőség, hogy a jelentkező profiloldalát a munkáltató lementse, tárolja vagy más számára továbbítsa.

A KOKI a különböző módokon beérkező pályázatokat a kiválasztási eljárás lezárultát követő 30 napig őrzi meg. Amennyiben a pályázó hozzájárul, a pályázati anyagát egy későbbi lehetséges álláslehetőséghez további 6 (Hat) hónapig őrzi meg.

10. A Társaság munkatársai által alkalmazandó általános adatkezelési szabályok

A Társaság valamennyi munkatársa köteles a személyes adatok kezelése vonatkozásában az alábbi gyakorlati szabályokat megtartani:

- A munkavégzés során csak az ahhoz elengedhetetlenül szükséges személyes adatok kezelhetők, továbbíthatók, az adott feladatot ellátó szervezeti egység vezetőjének felelőssége a munkafolyamatok ennek megfelelő kialakítása.
- Az informatikai jogosultságok engedélyezésekor figyelemmel kell lenni arra, hogy személyes adathoz csak az férhessen hozzá, akinek a munkavégzéséhez az az adat, adatkör elengedhetetlenül szükséges.
- Személyes adatot tartalmazó papír alapú dokumentum csak zárt borítékban továbbítható, illetve törekedni kell a személyes átadás megvalósulására.
- E-mailben személyes adatot tartalmazó dokumentum csak úgy továbbítható, hogy biztosított legyen, hogy azt csak az arra jogosult tekintheti meg, ennek érdekében — minimálisan — a személyes adatot csak a levél csatolmányaként lehet továbbítani, és a személyes adattartalomra utaló figyelmeztető mondatot kell elhelyezni a levél törzsszövegében a következők szerint: „A csatolmány személyes adatokat tartalmaz, ennek megismerésére csak és kizárólag a levél címzettje jogosult.”. A kiküldendő levelet a kiküldést megelőzően ellenőrizni kell, hogy a megfelelő e-mail címek szerepelnek-e a címzettek között
- A szervezeti egységek által használt közös meghajtókon személyes adatot tartalmazó dokumentum csak akkor tárolható, ha biztosított, hogy azt csak az arra jogosultak tekintik meg.

11. Különleges személyes adatok

A különleges adatok, vagyis 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 kezelése kizárólag a GDPR 9. cikk (2) bekezdésben felsorolt esetekben lehetséges.

12. Adatbiztonság

A KOKI mindent megtesz annak érdekében, hogy figyelembe véve a tudomány és technológia mindenkori állását, a megvalósítás költségeit, továbbá az adatkezelés jellegét, valamint a természetes személyek jogaira és szabadságaira jelentett kockázat a megfelelő technikai és szervezési intézkedéseket hajtson végre annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja.

A személyes adatokat mindig bizalmasan, korlátozott hozzáféréssel, titkosítással és az ellenálló képesség lehetséges maximalizálásával, probléma esetén visszaállíthatóság biztosításával kezeli. Rendszereit rendszeresen teszteli a biztonság garantálása érdekében. A biztonság megfelelő szintjének meghatározásakor figyelembe veszi az adatkezelésből eredő olyan kockázatokat, amelyek különösen a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítéséből, elvesztéséből, megváltoztatásából, jogosulatlan nyilvánosságra hozatalából vagy az azokhoz való jogosulatlan hozzáférésből erednek.

Megtesz mindent annak biztosítása érdekében, hogy az irányítása alatt eljáró, a személyes adatokhoz hozzáféréssel rendelkező személyek kizárólag utasításainak megfelelően kezelhessék az említett adatokat, kivéve, ha az ettől való eltérésre uniós vagy tagállami jog kötelezi őket.

A munkatársak és a KOKI 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.

A KOKI az elektronikus információs rendszerben tárolt adatok védelme körében gondoskodik különösen:

- az adminisztratív és a logikai védelmi intézkedésekről, beleértve a jogosulatlan hozzáférés elleni védelmet is,
- az adatállományok helyreállításának lehetőségét biztosító intézkedésekről, ezen belül a rendszeres biztonsági mentésről és a másolatok elkülönített, biztonságos kezeléséről,
- az adatállományok kártékony kódok elleni védelméről,
- az adatállományok, illetve az adatokat hordozó eszközök fizikai védelméről, ezen belül az objektumvédelmi intézkedések megtételéről, valamint a tűzkár, vízkár, villámcsapás, egyéb elemi kár elleni védelemről, illetve az ilyen események következtében bekövetkező károsodások helyreállíthatóságáról.

13. Biztonsági rendszerek

A KOKI által alkalmazott kamerák beállításának és használatának részletes szabályozását a Kamerarendszer Üzemeltetési Szabályzat tartalmazza, a beléptető rendszer alkalmazásának szabályait pedig az Adatkezelési tájékoztató beléptetőrendszerről.

14. Adatvédelmi incidens

Az adatvédelmi incidens akkor következik be, amikor az adat biztonsági előírásokat valaki szándékosan, vagy véletlenül nem tartja be és ennek eredményeképpen sérül a titoktartási kötelezettség, a hozzáférhetőség vagy az integritás. (pl. nyilvánosságra kerülnek e-mailcímek, telefonszámok vagy bankkártya adatok; elvesznek merevlemezek, akták, amelyeken személyes adatok szerepelnek; valaki feltöri az online rendszert, stb…)

Ha ez bekövetkezik és az incidens feltehetően kockázatot jelent az érintettek jogaira és szabadságaira nézve, indokolatlan késedelem nélkül, legkésőbb a tudomásra jutástól számított 72 (Hetvenkettő) órán belül, azt jelenteni kell a NAIH felé és általában értesíteni kell az érintetteket is.

A NAIH-nak 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 a Társaság 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 adatvédelmi tisztviselő elektronikusan nyilvántartja az adatvédelmi incidenseket, feltüntetve az adatvédelmi incidenshez kapcsolódó tényeket, annak hatásait és az orvoslására tett intézkedéseket.

Ha az incidens nem jelent nagy kockázatot, nem kell jelenteni a NAIH felé és nem kell értesíteni az érintetteket, de a hibát azonnal helyre kell hozni és fel kell vezetni az incidensek nyilvántartásába.

Az adatvédelmi incidensek kezeléséről az Incidenskezelési Szabályzat részletesen rendelkezik.

15. Nyilvántartási kötelezettség

A GDPR 30. cikke – az abban meghatározott tartalommal és kivételekkel - előírja, hogy a végzett adatkezelési tevékenységekről nyilvántartást kell vezetni melyet megkeresésre a

felügyeleti hatóság (NAIH) rendelkezésére kell bocsátani és az adatkezelés jogszerűségét ezáltal is igazolni.

A nyilvántartást legalább évente felül kell vizsgálni és aktualizálni. Valamennyi szervezeti egység feladta, hogy felülvizsgálja a saját területén alkalmazott eljárásokat és rendszereket és ahol szükségesnek látja módosításokat javasoljon.

Azonban a mennyiben a nyilvántartás módosítása évközben is szükségessé válik, azt az Adatvédelmi Tisztviselő felé jelezni kell.

16. Hatásvizsgálat

Ha az adatkezelés valamely — különösen új technológiákat alkalmazó — típusa, figyelemmel annak jellegére, hatókörére, körülményére és céljaira, valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, a KOKI az adatkezelést megelőzően hatásvizsgálatot végez arra vonatkozóan, hogy a tervezett adatkezelési műveletek a személyes adatok védelmét hogyan érintik.
Olyan, egymáshoz hasonló típusú adatkezelési műveletek, amelyek egymáshoz hasonló magas kockázatokat jelentenek, egyetlen hatásvizsgálat keretei között is értékelhetőek.
A hatásvizsgálatot az adott adatkezelést végző szervezeti egység köteles elvégezni az adatvédelmi tisztviselő közreműködésével.
A hatásvizsgálat lefolytatására a NAIH honlapjáról letölthető hatásvizsgálati szoftvert kell használni.

A hatásvizsgálat lefolytatását követően:

- A NAIH kérésére az adatvédelmi hatásvizsgálatról szóló jelentést be kell nyújtani a NAIH felé;
- Konzultálni kell a NAIH-hal, ha nem sikerült megfelelő intézkedéseket hozni a magas kockázatok csökkentésére;
- Rendszeresen, de legalább az adatkezelési művelettel járó kockázat megváltozása esetén felül kell vizsgálni az adatvédelmi hatásvizsgálatot és a tárgyát képező adatkezelést;
- Írásba kell foglalni a hatásvizsgálat alapján hozott döntéseket.

17. Adatfeldolgozók

Adatfeldolgozó az a cég vagy személy, amely vagy aki kizárólag technikai végrehajtást végez a KOKI utasításai alapján, önálló döntést az adatkezelés kapcsán nem hoz.

Az ilyen cégeket az együttműködő cégek nyilvántartásában fel kell tüntetni.

18. Közérdekű adatok

Az Infotv. 30.§ (6), 35. § (3), a 32. § - 37/B. § - ban foglaltak alapján, továbbá a közérdekű adatok elektronikus közzétételére, az egységes közadatkereső rendszerre, valamint a központi jegyzék adattartalmára, az adatintegrációra vonatkozó részletes szabályokról szóló 305/2005.

(XII. 25.) Korm. rendelet 3. §-ában és a közzétételi listákon szereplő adatok közzétételéhez szükséges közzétételi mintákról szóló 18/2005. (XII. 27.) IHM rendeletben foglaltaknak eleget téve a közérdekű adatok igénylésének rendje és a közérdekű és közérdekből nyilvános adatok közzétételének rendjére két külön szabályzat vonatkozik.

Jelen Szabályzatot kiadtam 2021. ……..- napján.

_____

Dr. Nusser Zoltán
igazgató