MAGYAR BÍRÓSÁGI VÉGREHAJTÓI KAR

3/2021. (09.20) SZÁMÚ

ADATVÉDELMI ÉS INCIDENSKEZELÉSI

SZABÁLYZATA

Dokumentum kontroll

Változások

Verzió	Kiadás dátuma	Kiadás célja / módosítás lényege
1.0	2021. szeptember 20.	Magyar Bírósági Végrehajtói Kar adatkezelési tevékenységeivel kapcsolatos jogainak és kötelezettségeinek, kiemelten teljesítendő szervezési, adminisztratív, logikai és fizikai védelmi intézkedési kötelezettségeinek meghatározása
2.0	2026. május 21.	A szabályzat felülvizsgálata és aktualizálása a hatályos jogszabályoknak és a szervezeti és működési változásoknak megfelelően

Kiadás

Készült	2 eredeti példányban

TARTALOMJEGYZÉK

1. BEVEZETŐ RENDELKEZÉSEK

A Magyar Bírósági Végrehajtói Kar (a továbbiakban: Kar, vagy Adatkezelő) a bírósági végrehajtásról szóló 1994. évi LIII. törvény (a továbbiakban: „Vht.") alapján létrejött jogi személy, amelyre a Vht.-ban meghatározott eltérésekkel a köztestületekre vonatkozó szabályokat kell alkalmazni. Adatkezelő az önálló bírósági végrehajtók szakmai és érdek-képviseleti szerveként a Vht.-ban, kiemelten annak 250. § (2) bekezdésében, és egyéb jogszabályokban meghatározott közérdekű feladatok ellátására jött létre, mely feladatokat a Vht. 250. § (3) bekezdése alapján hivatali szerve útján gyakorolja. A Vht. 250. § (7) bekezdésének megfelelően Kar közfeladatai ellátása kapcsán, illetve egyéb, közfeladat ellátásához kapcsolódó folyamatai során adatot kezel, így Adatkezelőként felel az adatvédelmi alapelveknek megfelelő joggyakorlás kialakításáért, az adatkezelés jogszerűségének biztosításáért.

Adatkezelési tevékenységgel járó folyamatainak hatékony és ésszerű tervezése és megszervezése, dokumentálása és nyilvántartása, a Kar által alkalmazott személyek feladat- és jogköreinek meghatározása, az érintettek adatvédelemmel kapcsolatos jogainak biztosíthatósága, és az adatvédelmi incidenskezelési eljárásrend kialakítása céljából Adatkezelő az alábbi Adatvédelmi és incidenskezelési szabályzatot (a továbbiakban: szabályzat) alkotja.

Adatkezelő megnevezése:	**Magyar Bírósági Végrehajtói Kar**
Adatkezelő rövidített elnevezés:	**MBVK**
Adatkezelő adószáma:	**18654714-1-42**
Adatkezelő székhelye:	**1146 Budapest, Cházár András u. 13.**
Telephelye:	**1146 Budapest, Hermina út 63.**
Adatkezelő adatvédelmi kérdésekben alkalmazott elektronikus elérhetősége:	**adatvedelem@mbvk.hu**
Adatkezelő hivatalos elektronikus elérhetősége:	**MBVK rövid nevű, 349507779 KRID azonosítójú hivatali kapu**
Adatkezelő képviselője:	**Dr. Takács Katalin Hivatalvezető**
Adatkezelő Adatvédelmi Tisztviselője:	**Dr. Erdélyi Dávid**

Jelen rendelkezéseket a Kar többi szabályzatának előírásaival összhangban kell értelmezni. Amennyiben a személyes adatok védelmével kapcsolatosan ellentmondás áll fent jelen rendelkezések és a bármely más, jelen szabályzat hatálybalépése előtt hatályba lépett szabályzat előírásai között, úgy abban az esetben jelen rendelkezések az irányadóak.

Jelen szabályzat az alábbi jogszabályokban meghatározottakkal együtt értelmezendő. A szabályzatban -e jogszabályok az itt rögzített rövidítésekkel kerülnek feltüntetésre.

Infotv.	az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény
GDPR	az Európai Parlament és a Tanács (EU) 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 2016/679 rendelete
NAIH	Nemzeti Adatvédelmi és Információszabadság Hatóság

2. ÁLTALÁNOS RENDELKEZÉSEK:

2.1. A SZABÁLYZAT CÉLJA ÉS HATÁLYA

A szabályzat megalkotásával a Kar biztosítani kívánja szervezetén belül azoknak a szervezési és technikai intézkedéseknek meghatározását, valamint - a szabályzatban meghatározottak alapján - azok kialakítását, alkalmazását, folyamatos ellenőrzését, és szükség esetén biztosítandó korrekcióját, mely intézkedésekkel az adatvédelem alapelveinek, a jogszerű adatkezelés feltételeink, az adatbiztonság követelményeinek érvényesülése megvalósítható. Adatkezelő az adatok biztonsági állapotának lehetséges sérülése esetén kötelezően elvégzendő vizsgálatra, a vizsgálat eredménye alapján lefolytatandó eljárásokra jelen szabályzatban cselekvési tervet határoz meg annak érdekében, hogy az adatvédelmi incidensek minden esetben azonos, magas színvonalon kerüljenek felderítésre, valamint a lehetséges kockázatok a lehető leghamarabb és leghatékonyabb módszerekkel csökkenthetőek legyenek, a Kar tevékenysége pedig megfeleljen a GPDR-ban meghatározott elvárásoknak és transzparenciának.

A szabályzat tárgyi hatálya kiterjed a Kar minden szervezeti egységénél folytatott valamennyi olyan folyamatra, amely során a GDPR 4. cikk 1. pontjában meghatározott személyes adat kezelése megvalósul.

Jelen szabályzat személyi hatálya kiterjed a Kar, mint Adatkezelő irányítása alatt eljáró, a személyes adatokhoz hozzáféréssel rendelkező természetes személyekre (a munkavégzésre irányuló jogviszony jellegétől függetlenül), és azon természetes személyekre (a továbbiakban: érintett), akik személyes adatait a jelen szabályzat hatálya alá tartozó adatkezelések feldolgozzák, továbbá azon érintettekre, akik jogait vagy jogos érdekeit az adatkezelési tevékenység érinti. A Kar megbízásából személyes adatok kezelését vagy feldolgozását végzők esetén az erre a jogviszonyra a Kar által kötött szerződésben a GDPR 28. cikkének megfelelően rendelkezni kell arról, hogy a Kar által megbízott adatfeldolgozó a feladata ellátása során hogyan juttatja érvényre jelen szabályzat rendelkezéseit (figyelembe véve a 1. mellékletben meghatározott adatvédelmi bekezdések, kiegészítések tartalmát), egyéb esetben az adatfeldolgozóval a Kar a GDPR által előírt Adatfeldolgozói szerződést köt (2. melléklet). A Kar szervezeti egységeinél adatkezelést végző alkalmazottak és a Kar megbízásából az adatkezelésben résztvevő, annak valamely műveletét végző szervezetek alkalmazottjai kötelesek a megismert személyes adatokat üzleti titokként megőrizni. A személyes adatokat kezelő és azokhoz hozzáférési lehetőséggel rendelkező személyek kötelesek Titoktartási nyilatkozatot tenni (3. melléklet).

Jelen szabályzat hatálya nem terjed ki a harmadik személyek, így különösen az egyes önálló bírósági végrehajtók adatkezeléseire.

2.2. FOGALMAK

Adatállomány: az Infotv. 3. § 21. pontja szerinti adatok *(„az egy nyilvántartásban kezelt adatok összessége");*

Adatfeldolgozás: az Infotv. 3. § 17. pont szerinti tevékenység *(„az adatkezelő megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által végzett adatkezelési műveletek összessége")*;

Adatfeldolgozó: a GDPR 4. cikk 8. pontja szerinti személy *(„az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel");*

Adatkezelés: GDPR 4. cikk 2. pontjában meghatározott tevékenység *(„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")*;

Adatkezelő: GDPR 4. cikk 7. pontjában meghatározott személy *(„az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza; ha az adatkezelés céljait és eszközeit az uniós vagy a tagállami jog határozza meg, az adatkezelőt vagy az adatkezelő kijelölésére vonatkozó különös szempontokat az uniós vagy a tagállami jog is meghatározhatja");*

Adatkezelés korlátozásához való jog: a GDPR 18. cikk (1) bekezdés szerinti érintetti jog *(„Az érintett jogosult arra, hogy kérésére az adatkezelő korlátozza az adatkezelést, ha az alábbiak valamelyike teljesül:*

a) az érintett vitatja a személyes adatok pontosságát, ez esetben a korlátozás arra az időtartamra vonatkozik, amely lehetővé teszi, hogy az adatkezelő ellenőrizze a személyes adatok pontosságát;
b) az adatkezelés jogellenes, és az érintett ellenzi az adatok törlését, és ehelyett kéri azok felhasználásának korlátozását;

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

d) *az érintett a 21. cikk (1) bekezdése szerint 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.");*

Adatmegsemmisítés: az Infotv. 3. § 16. pont szerinti tevékenység *(„az adatot tartalmazó adathordozó teljes fizikai megsemmisítése")*;

Adattovábbítás: Infotv. 3. § 11. pontjában meghatározott tevékenység *(„az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele");*

Adattörlés: Infotv. 3. § 13. pont szerinti tevékenység *(„az adat felismerhetetlenné tétele oly módon, hogy a helyreállítása többé nem lehetséges");*

Adatvédelmi incidens: az adatok biztonsági állapotának sérülése a GDPR 4. cikk 12. pont szerint *(„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");*

Álnevesítés: a GDPR 4. cikk 5. pontja szerinti tevékenység *(„a személyes adatok olyan módon történő kezelése, amelynek következtében további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik, feltéve, hogy az ilyen további információt külön tárolják, és technikai és szervezési intézkedések megtételével biztosított, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet kapcsolni");*

Az érintett hozzájárulása: GDPR 4. cikk 11. pont szerinti jognyilatkozat *(„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")*

Biometrikus adat: a GDPR 4. cikk 14. pontja szerinti adat *(„egy természetes személy testi, fiziológiai vagy viselkedési jellemzőire vonatkozó minden olyan sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását, ilyen például az arckép vagy a daktiloszkópiai adat")*;

Címzett: a GDPR 6. cikk 9. pontja szerinti személy *(„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");*

Egészségügyi adat: a GDPR 4. cikk 15. pontja szerinti 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")*;

EGT-állam: az Infotv. 3. § 23. pontja szerinti államok *(„az Európai Unió tagállama és az Európai Gazdasági Térségről szóló megállapodásban részes más állam, továbbá az az állam, amelynek állampolgára az Európai Unió és tagállamai, valamint az Európai Gazdasági Térségről szóló megállapodásban nem részes állam között létrejött nemzetközi szerződés alapján az Európai Gazdasági Térségről szóló megállapodásban részes állam állampolgárával azonos jogállást élvez");*

Személyes adat: a GDPR 4. cikk 1. pont szerinti („*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");*

Érintett joga: a GDPR 12-22. cikkében szabályozott jogok, azaz

- tájékoztatás joga,
- hozzáférési jog,
- helyesbítéshez való jog,
- törléshez való jog,

- adatkezelés korlátozhatóságához való jog,
- adathordozhatósághoz való jog,
- tiltakozáshoz való jog,
- automatizált döntéshozatallal kapcsolatos jogok.

Felügyeleti hatóság: egy tagállam által a GDPR 51. cikknek megfelelően létrehozott független közhatalmi szerv. Az Infotv. 38. § (2a) bekezdés alapján a GDPR-ban a felügyeleti hatóság részére megállapított feladat- és hatásköröket a Magyarország joghatósága alá tartozó jogalanyok tekintetében az általános adatvédelmi rendeletben, valamint az Infotv-ben meghatározottak szerint a NAIH gyakorolja;

Genetikai adat: a GDPR 4. cikk 13. pontja szerinti adat *(„egy természetes személy örökölt vagy szerzett genetikai jellemzőire vonatkozó minden olyan személyes adat, amely az adott személy fiziológiájára vagy egészségi állapotára vonatkozó egyedi információt hordoz, és amely elsősorban az említett természetes személyből vett biológiai minta elemzéséből ered")*;

Harmadik fél: a GDPR 4. cikk 10. pontja szerinti adat *(„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 kap*tak");

Harmadik ország: az Infotv. 3. § 24. pontja szerinti államok *(„minden olyan állam, amely nem EGT-állam")*;

Képviselő: a GDPR 6. cikk 17. pontja szerinti személy vagy szervezet *(„az az Unióban tevékenységi hellyel, illetve lakóhellyel rendelkező és az adatkezelő vagy adatfeldolgozó által írásban megjelölt természetes vagy jogi személy, aki, illetve amely az adatkezelőt vagy adatfeldolgozót képviseli az adatkezelőre vagy adatfeldolgozóra az e rendelet értelmében háruló kötelezettségek vonatkozásában")*;

Nyilvánosságra hozatal: az Infotv. 3. § 12. pont szerinti közzététel *(„az adat bárki számára történő hozzáférhetővé tétele")*;

Nyilvántartási rendszer: a GDPR 6. cikk 6. pontja szerinti rendszer *(„a személyes adatok bármely módon – centralizált, decentralizált vagy funkcionális, vagy földrajzi szempontok szerint – tagolt állománya, amely meghatározott ismérvek alapján hozzáférhető")*;

Profilalkotás: a GDPR 6. cikk 4. pontja szerinti tevékenység *(„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 előre jelzésére használják")*;

Releváns és megalapozott kifogás: a GDPR 6. cikk 24. pontja szerinti joggyakorlás *(„a döntéstervezettel szemben benyújtott, azzal kapcsolatos kifogás, hogy ezt a rendeletet megsértették-e, illetve, hogy az adatkezelőre vagy az adatfeldolgozóra vonatkozó tervezett intézkedés összhangban van-e a rendelettel; a kifogásban egyértelműen be kell mutatni a döntéstervezet által az érintettek alapvető jogaira és szabadságaira, valamint adott esetben a személyes adatok Unión belüli szabad áramlására jelentett kockázatok jelentőségét")*;

Személyes adat: GDPR 4. cikk 1. pont szerinti 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")*;

Személyes adat különleges kategóriái: GDPR 9. cikk 1. pontja szerinti adat *(„Személyes adat különleges kategóriái: 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")*;

Tiltakozás: GDPR 21. cikk (1) bekezdésben meghatározott joggyakorlás *(„az érintett jogosult arra, hogy saját helyzetével kapcsolatos okokból bármikor tiltakozzon személyes adatainak a GDPR 6. cikk (1) bekezdésének e) vagy f) pontján alapuló kezelése ellen, ideértve az említett rendelkezéseken alapuló profilalkotást is")*.

2.3. Az adatkezelések irányelvei, jogszerűsége

A Kar felelős a személyes adatok kezelésére vonatkozó, a GDPR 5. cikk (1) bekezdésében meghatározott alapelvek betartásáért és érvényesítésért. A Karnak képesnek kell lennie a személyes adatok kezelésére vonatkozó alapelvek

betartásának igazolására a GDPR 5. cikk (2) bekezdésének megfelelően. A megfelelőség igazolása különösen az adatkezeléshez kapcsolódó döntéseket megalapozó körülmények és a döntések (pl. az adatkezelés feltételeit meghatározó döntéselőkészítő iratok), az érintetteknek szóló adatkezelési tájékoztatók, az érintettől származó nyilatkozatok (pl. hozzájáruló nyilatkozatok, az adatkezelési tájékoztató megismerését igazoló dokumentumok), továbbá a személyes adatokat tartalmazó (elektronikus vagy papír alapú) dokumentumok szervezeten belüli vagy azon kívüli mozgásának megfelelő dokumentálásával történik. A Kar – a GDPR 30. cikkének megfelelően – nyilvántartást vezet az általa végzett adatkezelésekről (a továbbiakban: adatkezelési tevékenységek nyilvántartása).

A megfelelőség igazolására az adatvédelmi incidensekről, és az érintetti joggyakorlás teljesítésének körülményeiről nyilvántartást vezet. Adatvédelmi incidens esetén különösen az incidenssel érintettek körének, az incidenssel érintett személyes adatok körének, az incidens kezelése során tett intézkedéseket megalapozó körülmények és a döntések dokumentálásával történik. A Kar – a GDPR 33. cikkének megfelelően – nyilvántartást vezet a bekövetkezett incidensekkel kapcsolatos tényekről és intézkedésekről (a továbbiakban: adatkezelési incidensek nyilvántartás). Érintetti joggyakorlásra vonatkozó megkeresés esetén különösen az adatigénylés tárgyát, dátumát, az érintett személyes adatok körét, az adatszolgáltatásra vonatkozó körülményeket, a megkeresésre adott mindennemű kommunikációt tartja nyilván az Adatkezelő (Érintetti joggyakorlás nyilvántartása).

A Kar felelős a személyes adatok kezelésének jogszerűségét biztosítani (GDPR 6. cikk). Személyes adatok kezelése akkor jogszerű, ha a GDPR szerinti jogalapja meghatározható (GDPR 6. cikk (1) bekezdés), személyes adatok különleges kategóriáinak minősülő adatok esetén az általános adatkezelésre vonatkozó tiltás alól (GDPR 9. cikk (1) bekezdés) a Kar rendelkezik a GDPR 9. cikk (2) bekezdése szerinti felmentéssel. A Kar a jogszerűség megalapozottságát, folyamatos fennállását az adatkezelés minden fázisában ellenőrzi, meghatározott időnként felülvizsgálja, és az egyes adatkezelési tevékenységek nyilvántartó lapjain dokumentálja.

A szervezet nevében adatkezelést végző alkalmazottak kártérítési, szabálysértési- és büntetőjogi felelősséggel tartoznak a személyes adatok jogszerű kezeléséért. Amennyiben az alkalmazott tudomást szerez arról, hogy az általa kezelt adat hibás, hiányos, időszerűtlen, köteles azt helyesbíteni, vagy a helyesbítést az adat rögzítéséért felelős munkatársnál kezdeményezni.

3. RÉSZLETES RENDELKEZÉSEK

3.1. AZ ADATVÉDELMI TEVÉKENYSÉG SZERVEZETE ÉS IRÁNYÍTÁSA

Az adatvédelmi tevékenység irányításában és ellátásában a Kar szervezeti egységei – a Szervezeti és Működési Szabályzatban meghatározott feladatkörükön belül – az alábbiak szerint vesznek részt.

3.1.1. Elnökség:

Az Elnökség felelős azért, hogy

3.1.1.1. a végrehajtókkal és a Karral kapcsolatos jogszabály tervezetek véleményezése során az adatvédelmi alapelvek érvényesítése már a tervezetek tartalmában is megjelenjen;

3.1.1.2. a Kar érdek-képviseleti tevékenysége keretei között lehetőséget biztosítson a tagok közötti adatvédelmi szakmai egyeztetéseknek, ágazat joggyakorlat egységesítő törekvéseinek;

3.1.1.3. a sajtó képviselőivel történő kapcsolattartás során a végrehajtói titoktartási kötelezettség érvényesítésre kerüljön;

3.1.1.4. adatvédelmi incidens esetén – az Adatvédelmi Tisztviselő közreműködésével és javaslata alapján – kiadott sajtóközlemény a GDPR szerinti cél elérésére alkalmas legyen.

3.1.2. Hivatalvezető:

A Hivatalvezető felelős azért, hogy a Kar – mint adatkezelő, illetve adatfeldolgozó – működése az adatvédelmi szabályoknak megfeleljen. Ennek érdekében:

3.1.2.1. gondoskodik az adatvédelmi tevékenység irányításában és ellátásában résztvevő szervezeti egységek kijelöléséről, feladataik, az adatvédelmi tárgyú ügyekkel kapcsolatos döntési jogkörök meghatározásáról, az egyes adatkezelési döntési szintek kialakításáról;

3.1.2.2. biztosítja az adatvédelmi tevékenység irányításához és ellátásához, valamint az érintett jogai gyakorlásához szükséges személyi és tárgyi feltételeket;

3.1.2.3. felelős az adat- és titokvédelmi, valamint biztonsági és információbiztonsági szabályzatok kiadásáért és betartatásáért;

3.1.2.4. gondoskodik az adatvédelmi tevékenység során esetleg előforduló, feltárt hiányosságok megszűntetéséről, szükség szerint a felelősségre vonásról;

3.1.2.5. kinevezi a Kar Adatvédelmi Tisztviselőjét, és az Adatvédelmi Tisztviselő nevét és elérhetőségét bejelenti a NAIH-nak;

3.1.2.6. munkajogi értelemben vett közvetlen felettese az Adatvédelmi Tisztviselőnek.

3.1.3. Irodavezetők, csoportvezetők:

A Kar szervezeti egységeinek vezetői (irodavezető, csoportvezető) az irányításuk alá tartozó szervezeti egység tekintetében:

3.1.3.1. betartják és betartatják az adat- és titokvédelmi, valamint a biztonsági és információbiztonsági előírásokat;

3.1.3.2. az Adatvédelmi Tisztviselővel, a Jogi Irodával, Informatikai Irodával, valamint az Gazdasági és Pénzügyi Irodával együttműködve gondoskodnak az adat- és titokvédelmi, valamint a biztonsági és információbiztonsági előírások, szabályzatok megismertetéséről, rendszeres oktatásáról a 4. mellékletben foglaltaknak megfelelően;

3.1.3.3. gondoskodnak arról, hogy az irányításuk alá tartozó szervezeti egységek felelősségi körébe tartozó nyilvántartási rendszerek naprakészek, megbízhatóak legyenek;

3.1.3.4. gondoskodnak arról, hogy az irányításuk alatt álló személyek az adatkezelés meghatározott feltételeinek megfelelően járjanak el (GDPR 32. cikk (4) bekezdés).

3.1.4. Hivatali Titkárság:

A Hivatali Titkárság a feladatkörében:

3.1.4.1. gondoskodik a papír alapú dokumentumok iratkezelése során jelen szabályzatban meghatározottak érvényesüléséről;

3.1.4.2. felelős a Kar által szervezett oktatások, rendezvények kapcsán, valamint a lapkiadó tevékenység gyakorlása során az adatkezelési tevékenységekkel kapcsolatosan meghatározott folyamatok, és jelen szabályzatban meghatározott elvek gyakorlati alkalmazásáért az Adatvédelmi Tisztviselő szükség szerinti közreműködésével.

3.1.5. Ügyfélszolgálati és Panasz Iroda:

Az Ügyfélszolgálati és Panasz Iroda a feladatkörében:

3.1.5.1. az Adatvédelmi Tisztviselő részére továbbítja az érintetti jogok gyakorlásával kapcsolatos, valamint a lehetséges incidensekkel kapcsolatos beadványokat, valamint a személyes adatok kezelését, illetve a GDPR szerinti jogaik gyakorlását érintő érintetti panaszokat;

3.1.5.2. panasznapon, telefonos megkeresés esetén gondoskodik arról, hogy a szóban vele közölt személyes adatnak minősülő információhoz illetéktelenek ne férhessenek hozzá;

3.1.5.3. kiemelt figyelmet fordít arra, hogy szóban, az érintett azonosítása nélkül személyes adatot ne közöljön a megkeresőkkel.

3.1.6. Informatikai Iroda:

Az Informatikai Iroda a feladatkörében:

3.1.6.1. ellátja az informatikai fejlesztéseknél és beszerzéseknél a beépített adatvédelem kontrolljai meglétének biztosításával, az adatminőség biztosításával, az informatikai biztonság kockázatarányos szintjét biztosító jogosultsági és naplózási rendszer kialakításának megfelelőségével, a biztonságos szoftverfejlesztés alapelveinek érvényesítésével kapcsolatos feladatokat;

3.1.6.2. az informatikai rendszerek üzemeltetése területén ellátja a személyes adatok kezelésével kapcsolatos technikai védelem megvalósítását;

3.1.6.3. ellátja – a Kar Informatikai Biztonsági Szabályzatában meghatározott – hatáskörébe tartozó információbiztonsági feladatokat, valamint rendelkezésre állási kontrollok biztosítását, a tárolt és továbbított személyes adatok bizalmasságának védelmét, az incidensfelderítési és - kezelési tevékenység támogatását;

3.1.6.4. az érintett szervezeti egységek vezetőivel együttműködve gondoskodik az információbiztonsági előírások, szabályzatok megismertetéséről, rendszeres oktatásáról.

3.1.7. Információbiztonsági Felelős:

Az Információbiztonsági Felelős feladatkörében:

3.1.7.1. együttműködik az Adatvédelmi Tisztviselővel és az adatkezelést végző szakterületekkel az adatkezelések adatbiztonsági feltételeinek kialakítása során, az alkalmazható fizikai, logikai, adminisztratív védelmi megoldásokról javaslatot tesz, támogatja a beépített adatvédelem technikai feltételeinek kialakítását;

3.1.7.2. új informatikai rendszer bevezetése, informatikai rendszerrel kapcsolatos változások esetén tájékoztatja az Adatvédelmi Tisztviselőt tervezett rendszerről, változásokról, intézkedésekről;

3.1.7.3. informatikai incidens észlelése esetén haladéktalanul értesíti az Adatvédelmi Tisztviselőt, biztosítva, hogy a személyes adatokkal kapcsolatos érintettség vizsgálatát elvégezhesse;

3.1.7.4. adatvédelmi incidens észlelésekor a kivizsgálási, kockázat csökkentési, értékelési folyamatban aktívan közreműködik.

3.1.8. Jogi Iroda:

A Jogi Iroda a feladatkörében:

3.1.8.1. biztosítja a Kar Adatvédelmi Tisztviselője feladatainak ellátásához szükséges személyi és tárgyi feltételeket;

3.1.8.2. szakmai támogatást nyújt az adatkezeléssel összefüggő, nem adatvédelmi jogszabályok értelmezésében;

3.1.8.3. biztosítja, hogy az Adatvédelmi Tisztviselő véleményét kikérjék a Kar adatvédelmi tárgyú vagy adatvédelmi vonatkozású belső szabályzatainak előkészítése során;

3.1.8.4. biztosítja a Kar képviseletét az érintett által a Kar ellen az érintett adatvédelmi jogainak megsértése miatt indított, illetve a Kar által a NAIH határozatainak felülvizsgálata iránt indított perekben, illetve egyéb eljárásokban.

3.1.9. Ellenőrzési és Fegyelmi Iroda:

Az Ellenőrzési Iroda és Fegyelmi Iroda a feladatkörében:

3.1.9.1. kiemelt figyelmet fordít arra, hogy az ellenőrzések során rá bízott végrehajtói adatvagyonhoz semmilyen körülmények között ne férjen hozzá illetéktelen személy, a megőrzési idők lejáratakor az állományok törlése dokumentáltan végrehajtásra kerüljön az Adatvédelmi Tisztviselő bevonásával;

3.1.9.2. az ellenőrzések során feltárt, informatikai rendszerek működéséből eredő lehetséges adatvédelmi kockázatokat az Adatvédelmi Tisztviselő felé írásban visszajelezze.

3.1.10. Gazdasági és Pénzügyi Iroda:

A Gazdasági és Pénzügyi Iroda a feladatkörében:

3.1.10.1. biztosítja, hogy az Adatvédelmi Tisztviselő minden személyes adat kezelésével járó beszerzésről, szerződéskötésről tudomással rendelkezzen;

3.1.10.2. a költségvetés tervezésekor az adatvédelemmel kapcsolatos kiadásokra is elegendő forrást biztosít.

3.1.11. Adatvédelmi Tisztviselő:

Az Adatvédelmi Tisztviselőt a Hivatalvezető nevezi ki a Karral foglalkoztatási jogviszonyban álló természetes személyek közül. Adatvédelmi Tisztviselőnek olyan személy nevezhető ki, aki ismeri a Kar működését, feladatait, munkafolyamatait és rendelkezik:

- jogi végzettséggel, vagy informatikai főiskolai (BSc) vagy egyetemi (MSc) szintű végzettséggel;
- az európai és hazai adatvédelemmel kapcsolatos főbb szabályozók, hatósági és bírósági határozatok, iránymutatások ismeretével;
- alapvető adatvédelmi és informatikai folyamatok ismeretével.

Az Adatvédelmi Tisztviselő kinevezése mellett a Kar adatvédelmi tanácsadási feladattal egyéb, jogi vagy természetes személy szakértőt is megbízhat.

Az Adatvédelmi Tisztviselő független. Függetlensége biztosítása érdekében adatvédelmi tisztviselői szakmai feladatai ellátása során utasítást nem fogadhat el, szakmai feladatai jogszerű ellátásával összefüggésben nem bocsátható el. Jelen szabályzatban foglalt tevékenysége ellátása során autonóm, szakmai ügyekben kizárólag a Hivatalvezetőnek tartozik felelősséggel.

A Kar elősegíti az Adatvédelmi Tisztviselő megfelelő szakmai feladatellátását. Ennek érdekében a Kar biztosítja különösen a személyes adatokhoz és az adatkezelési műveletekhez való hozzáférést, valamint a szakértői szintű ismereteinek fenntartásaihoz szükséges forrás biztosítását, elegendő idő biztosítását feladatai ellátásához, valamint az informatikai és a biztonsági szakterület együttműködése révén az Adatvédelmi Tisztviselő bevonását:

- a megfelelő technikai-eljárási intézkedésekhez szükséges források meghatározása (költségvetési tervezés) során annak érdekében, hogy teljesüljenek az adatvédelem alapelvei a technikai vívmányok alkalmazása (beépített adatvédelem) és az adatvédelem-barát megoldások (alapértelmezett adatvédelem) révén;
- a felügyeleti szervvel történő együttműködés során, amellyel az Adatvédelmi Tisztviselő – a Jogi Iroda és az ügy természetéből adódóan esetenként egyéb szakterület munkatársainak bevonásával – tartja a kapcsolatot.

Az Adatvédelmi Tisztviselő véleményét – a jelen szabályzat rendelkezései szerint – ki kell kérni az adatkezelést érintő döntések, szerződések és belső szabályzatok tervezetéről.

Az Adatvédelmi Tisztviselőt tisztsége fennállása alatt és annak megszűnését követően titoktartási kötelezettség terheli a tevékenysége során tudomására jutott, közérdekű vagy közérdekből nem nyilvános adatnak nem minősülő információk kapcsán.

Nem lehet Adatvédelmi Tisztviselő az a természetes személy, aki az adatkezelési tevékenység céljainak, kereteinek, eszközeinek meghatározásáról dönt, különösen a Hivatalvezető, az Információbiztonsági felelős és az Informatikai Iroda vezetője.

Az Adatvédelmi Tisztviselő az Adatvédelmi Tisztviselői feladatokon kívül a Hivatalvezető döntése alapján más munkakörhöz kötődő feladatokat is elláthat, amennyiben azok nem eredményeznek összeférhetetlenséget.

Az Adatvédelmi Tisztviselő nevét és elérhetőségeit a Kar honlapján, székhelyén, telephelyén a nyilvánosság részére mindenkor elérhetővé kell tenni. A Kar továbbá közli az Adatvédelmi Tisztviselő nevét és elérhetőségét a NAIH-al.

Az Adatvédelmi Tisztviselő feladatai:

- közreműködik, illetve segítséget nyújt az adatkezeléssel összefüggő döntések meghozatalában, valamint az érintettek jogainak biztosításában;
- ellenőrzi a GDPR, az Infotv. és az adatkezelésre vonatkozó más jogszabályok, valamint a jelen szabályzat, továbbá a Kar egyéb belső szabályzatai rendelkezéseinek a megtartását;
- legalább 2 évente belső adatvédelmi ellenőrzési eljárást folytat le minden szakterületen;
- kivizsgálja – az érintett szakterületek és a Jogi Iroda bevonásával – a neki címzett panaszokat, jogszerűtlenség észlelése esetén annak megszüntetésére, korrekciós intézkedés megtételére hívja fel az adatkezelést végző vagy az adatfeldolgozót;
- elkészíti, és időszakosan felülvizsgálja és szükség esetén aktualizálja az Adatvédelmi és incidenskezelési szabályzatot;
- a Jogi Irodával együttműködve gondoskodik az adatvédelmi ismeretek oktatásáról;
- személyes adatot is kezelő új informatikai rendszer belső fejlesztéssel történő bevezetése során elvégzi az adatvédelmi hatásvizsgálatot;
- az adatvédelmi incidenskezeléssel kapcsolatban ellátja a jelen szabályzat szerinti feladatokat;
- vezeti az Adatkezelési Nyilvántartást;
- éves összefoglaló jelentést készít a Hivatalvezetőnek;
- kapcsolatot tart és – a Jogi Irodával, valamint az ügy természetéből adódóan esetenként egyéb szakterület munkatársainak bevonásával – együttműködik a NAIH-al;
- a NAIH kérésére adatszolgáltatást teljesít;
- gondoskodik a Jogi Irodával együttműködve az éves adatvédelmi és incidenskezelési oktatás szervezéséért a 4. mellékletben meghatározottak szerint;
- gondoskodik a közérdekű adatigénylések teljesítéséről, valamint támogatja az Elnökséget és a Hivatalvezetőt a sajtókapcsolati feladatainak ellátásában.

3.2. ADATVÉDELMI OKTATÁS:

Az Adatvédelmi Tisztviselő a Gazdasági- és Pénzügyi Irodával, valamint a Jogi Irodával együttműködve gondoskodik az adatvédelmi tudatosság növelése céljából évente tartandó adatvédelmi és incidenskezelési oktatás szervezéséről. Az oktatások során általános, betekintő jellegű adatvédelmi ismereteket, speciálisan az irodák napi tevékenységi körébe tartozó adatkezelések kapcsán felfrissítő jellegű folyamatismertetést, valamint az adatvédelmi incidensekkel kapcsolatos oktatást tart. Az adatvédelmi incidensek kapcsán ismerteti a múltban bekövetkezett adatvédelmi incidensek tapasztalatait, vagy a lehetséges adatvédelmi incidensek veszélyeit elemzi, a kockázatok csökkentésével, megelőzésével kapcsolatosan tájékoztatást ad, illetve az ismereteket ellenőrzi. Az éves oktatáson való részvétel minden Kar által munkaviszonyban foglalkoztatott személy részére kötelező.

3.3. ADATKEZELÉSI TEVÉKENYSÉG FÁZISAI:

Az adatkezelési tevékenységek fázisai:

3.3.1. adatkezelési tevékenység bevezetése,

3.3.2. adatkezelési tevékenység aktív alkalmazása,

3.3.3. adatkezelési tevékenység megszűntetése.

3.3.1. Általános szabályok:

Az egyes adatkezelési fázisokban jelen pontok szerinti folyamatok alkalmazása szükséges az adatkezelés alapelveinek hatékony alkalmazásához. Minden folyamatot dokumentálni szükséges az 5. melléklet szerinti adatkezelési tevékenység nyilvántartó lap nyomtatványon. A végleges dokumentumok szakmai megfelelőségéért a dokumentum létrehozását kezdeményező szakterület, az adatvédelmi megfelelőségéért az Adatvédelmi Tisztviselő, az informatikai, információbiztonsági megfelelőségért pedig az Információbiztonsági Felelős a felelős. Abban az esetben, ha bármely terület eltér a megfogalmazott szakmai, adatvédelmi vagy információbiztonsági állásfoglalásoktól, az eltérésért, illetve a végleges dokumentumért az eltérő szakterületi vezető tartozik felelősséggel.

Az adatkezelési tevékenységgel kapcsolatos változást tartalmazó nyilvántartó lapot - kitöltést követően - az Adatvédelmi Tisztviselő véleményezésre valamennyi irodavezető részére megküldi, az Irodavezetők véleményüket az Adatvédelmi Tisztviselő által meghatározott határidőben kötelesek visszaküldeni, amely nem lehet kevesebb 5 munkanapnál. A véleményeket az Adatvédelmi Tisztviselő összesíti és véglegesíti, szükség esetén az Irodavezetőkkel és a véleményezőkkel való konzultáció után, megőrzéséről az adatkezelési tevékenységek nyilvántartásával egy helyen gondoskodik.

Amennyiben az adatkezeléssel kapcsolatos változások feltételeinek kidolgozásában a részt vevők között véleményeltérés van, illetve a Jogi Iroda vagy az Informatikai Iroda kifogást fogalmaz meg az abban foglaltakkal kapcsolatban, az Adatvédelmi Tisztviselő – szükség esetén az adatkezelést végző szakterület irodavezetőivel és a véleményezőkkel való konzultáció után – javaslatot tesz a lehetséges megoldásra. Változás átvezetése kizárólag akkor kezdeményezhető, ha a konzultációs eljárásban minden résztvevő számára elfogadható megállapodás kialakítható a tervezett változásról.

Az Adatvédelmi Tisztviselő véleményét az adatkezelés bevezetéséről való döntést kezdeményező előterjesztésben ismertetni kell. Adatkezelési tevékenység bevezetése, változás bevezetése, vagy adatkezelési tevékenység megszűntetése kizárólag a nyilvántartó lapon átvezetett változás Hivatalvezetői elfogadását követően történhet.

3.3.2. Adatkezelési tevékenység bevezetése:

Jogszabályban elrendelt, jogszabály rendelkezése miatt szükséges, vagy a Kar döntése alapján létrehozandó, személyes adatokat kezelő nyilvántartás bevezetése esetén (ideértve a meglévő nyilvántartási rendszer adatainak új célú felhasználásával, új célú adatkezelés bevezetésével, nyilvántartási rendszerbe adatok felvételével, adatok tárolásával, harmadik személynek továbbításával

stb. járó adatkezelési tevékenység megkezdését is) bevezetése során az alábbi folyamat alkalmazása szükséges.

Adatkezelés bevezetése során az adatkezelési tevékenységet végző szervezeti egységnek az Adatvédelmi Tisztviselővel együttműködve meg kell határozni:

- az adatkezelési tevékenység tervezett folyamatát,
- a Kar adatkezelésben betöltött szerepét (Adatkezelőként, más adatkezelővel együtt Közös adatkezelőként, Adatfeldolgozóként végzi a műveleteket),
- az adatkezelésért felelős szervezeti egységnek és egyéb szervezeti egységeknek az adatkezeléssel kapcsolatos feladatait, így az adatok felvételének, módosításának, törlésének rendjét,
- egyéb nyilvántartásban szereplő adatok további felhasználása esetén meg kell határozni, hogy az eltérő célú adatkezelés összeegyeztethető-e az adatkezelés eredeti céljával, és így annak jogalapja szolgálhat-e a tervezett adatkezelés új jogalapjául [GDPR 6. cikk (4) bekezdés];
- az adatkezelés lényeges körülményeit érintően:
  - meg kell határozni az adatkezelés jogalapját, meghatározva szükség szerint feltüntetve a jogalapot alátámasztó jogszabályt, jogos érdeket, szerződést, létfontosságú érdeket, adatkezelés célját, megőrzési idejét, kezelendő adatkategóriákat, lehetséges érintettek kategóriáit;
  - vizsgálni kell, hogy a tervezett adatgyűjtés a célhoz kötött adatkezelés és az adattakarékosság elvének megfelelő -e;
  - meg kell határozni az adatkezelési tevékenység során szükséges adatszolgáltatási kötelezettségeket;
  - meg kell jelölni a nyilvántartási rendszerből történő adattovábbítás, az ahhoz való hozzáférés rendjét, azoknak a munkavállalóknak, egyéb címzetteknek a körét, akik részére a kezelendő személyes adatok továbbíthatók;
  - vizsgálni kell, hogy történik-e EGT térségen kívülre adattovábbítás, ha igen, melyik országba;
  - vizsgálni kell az egyéb, adatkezelés bevezetéséhez eldöntendő eseti feltételek teljesíthetőségét, fennállását;
  - az adatkezeléssel járó folyamatokra vonatkozó, és a gyakorlatban alkalmazott általános adatbiztonsági intézkedéseket, kiemelten az adatok sértetlenségével, bizalmasságuk megőrzésével és üzletmenet-folytonossággal kapcsolatos kontrollokat (pl. változáskezelés, rendelkezésre állás, jogosultságkezelés, adatrejtő eljárások, incidenskezelés támogatása);
  - beépített adatvédelem elvének érvényesítésére alkalmazott technikai megoldásokat az Informatikai Irodavezető, valamint az Információbiztonsági Felelős közreműködésével;
  - az Informatikai Irodavezető, valamint az Információbiztonsági Felelős közreműködésével azt, hogy az adatkezelés minden fázisa során biztosítható -e az események, változások automatikus dokumentálása (naplózás), amennyiben ez biztosítható, ezek milyen szabályrendszer alapján kerüljenek alkalmazásra;
  - amennyiben az adatkezelés során az Érintett jognyilatkozatot tesz, ennek tárolása visszakereshető formában hogyan valósul meg;
  - az adatkezelés automatizált döntéshozatali módszerrel történik, illetve profilalkotási módszer alkalmazására sor kerül -e [GDPR 22. cikk (1) bekezdés].

Az adatkezelés legfontosabb körülményeinek tisztázását követően az Adatvédelmi Tisztviselő feladata:

- előkészíteni az adatkezelési tájékoztatókat, nyilatkozatokat, érdekmérlegelési tesztet, hatásvizsgálatot, az adatkezelési tevékenységek között nyilvántartásba kell vennie az adatkezelési tevékenységet;
- hozzájáruláson alapuló adatkezelés esetén a hozzájáruló nyilatkozat mintájának, szerződéses kötelezettség esetén a szerződésben rögzítendő adatkezelésre vonatkozó szakaszok előkészítése;
- felmérni, hogy egyéb kapcsolódó nyomtatványon, tájékoztató dokumentumban szükséges -e az adatkezeléssel kapcsolatos tájékoztató módosítása, vagy az elkészült tájékoztató dokumentumok közzététele;

- gondoskodni arról, hogy az adatkezelésről készített érintetti tájékoztatás az mbvk.hu honlapon - vagy amennyiben az új adatkezelési tevékenység bevezetés kizárólag a Kar munkavállalóit érinti - a munkavállalói adatkezelési tájékoztatóban a Kar belső intranet felületén kerüljön közzétételre;
- amennyiben ennek szükségessége felmerül, egyedi esetben előterjesztést tesz a Hivatalvezetőnek arról, hogy személyes adatok harmadik országba továbbíthatók-e.

Amennyiben az új adatkezelés bevezetése elektronikus információs rendszert érint, az Informatikai Irodavezető, és az Információbiztonsági Felelőst is be kell vonni a folyamatba. Az új adatkezelés bevezetési igényt megfogalmazó szervezeti egység vezetője az egyéb területek érintett munkavállalói bevonásának szükségességéről gondoskodik.

Az adatkezelés feltételeinek kidolgozásában érintett szakterületek/szervezeti egységek vezetői kötelesek egymással és az Adatvédelmi Tisztviselővel együttműködni. A kidolgozás koordinálásáról az Adatvédelmi Tisztviselő gondoskodik.

3.3.3. Adatkezelési tevékenységek alkalmazása (aktív szakasz):

Az adatkezelésért felelős szervezeti egység feladatkörébe tartozó kérdésekben:

- képviseli az adatkezelőt az adatfeldolgozó felé vagy – közös adatkezelés esetén – a többi adatkezelő felé (amennyiben releváns);
- figyelemmel kíséri az adatkezelés feltételeinek folyamatos fennállását (beleértve az adatkezelés jogszerűségéhez szükséges tájékoztatások megadását, nyilatkozatok beszerzését stb.) és szükség esetén megteszi vagy kezdeményezi a szükséges intézkedéseket az adatkezelés feltételeinek módosítása iránt;
- gondoskodni köteles az adathordozók tekintetében a fizikai védelmi mechanizmusok alkalmazásáról (zárható szekrényekben tárolás, iratkezelési szabályzatban meghatározottak követése, fizikai adathordozók védelme stb.)

Az Adatvédelmi Tisztviselő feladatkörébe tartozik az adatkezelési tevékenység aktív szakaszában:

- a hozzájáruláson alapuló adatkezelések esetében annak ellenőrzése, hogy az érintett a hozzájárulását szabályosan szerezte-e be [GDPR 7. cikk (1) bekezdés];
- annak ellenőrzése és monitorozása, hogy a szervezeti egységek legalább az Érintettel való első kapcsolatfelvételkor biztosítják-e az adatkezelési tájékoztató megtekinthetőségét vagy annak online elérhetőségét;
- rendszeres időközönként, de legalább évente a hatásvizsgálatban azonosított kockázatok alakulásának áttekintése, a kockázatok változásának folyamatos monitorozása, a hatásvizsgálatok utóellenőrzése [GDPR 35. cikk (11) bekezdés],
- az adatkezelés feltételeinek módosítása esetén kapcsolatot tart az érintett szervezeti egységekkel, a változásokat rögzíti az adatkezelési tevékenység nyilvántartó lapjára, és az adatkezelési tevékenységek nyilvántartásába.

Változás az adatkezelési tevékenységben az aktív szakaszban: amennyiben az adatkezelési tevékenység aktív szakaszában szükséges valamilyen adatkezelési körülmény módosítása az érintett szervezeti egység az Adatvédelmi tisztviselő koordinációjával a szükséges intézkedéseket ismételten elvégzi, és dokumentálja az adatkezelést nyilvántartó lapon.

3.3.4. Adatkezelés megszüntetésével kapcsolatos feladatok:

Amennyiben a kezelt adatokra a továbbiakban nincs szükség (az adatkezelési cél megvalósult, vagy megszűnt), vagy jogszabályi változások miatt, illetve az adatvédelmi felügyeleti hatóság vagy bíróság döntése értelmében az adatok kezelését meg kell szüntetni, az adatkezelést végző szakterület – az Adatvédelmi Tisztviselő és rajta keresztül a Jogi Iroda és az Informatikai Iroda véleményének kikérése után – az adatkezelési nyilvántartó lapon javaslatot tesz a Hivatalvezetőnek:

- az adatkezelés egészének vagy egyes adatfajták nyilvántartásának megszüntetésére (vagy az adatok archiválására, illetve álnevesítésére az adattörlési idő leteltéig),
- a nyilvántartási rendszer egészének vagy egyes adatfajták, illetve adatok törlésére, vagy álnevesítésére.

- Adatkezelési tevékenység megszüntetésekor az Adatvédelmi Tisztviselő koordinálásával az együttműködő szakterületeknek:
- fel kell mérni az adatkezelési tevékenység megszüntetésével járó következményeket,
- az Adatkezelési Nyilvántartásból az adatkezelést vagy az egyes adatfajtákat törölni kell,
- az adatokat az informatikai rendszerekben archiválni, vagy álnevesíteni kell, illetve
- az informatikai rendszerekből törölni kell, a papír alapú nyilvántartásban kezelt adatokat pedig – a Kar iratkezelési szabályzatáról szóló utasítás szerint – selejtezni kell,
- jogszabály eltérő rendelkezése hiányában értesítenie kell az érintetteket.

3.4. ÉRDEKMÉRLEGELÉS:

3.4.1. Általános rendelkezések:

Amennyiben az adatkezelési tevékenység végzése a Kar, vagy harmadik fél jogos érdekére alapozható (GDPR 6. cikk (1) bekezdés f) pontja), az adatkezelési folyamat akkor és annyiban lesz jogszerű, amennyiben az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé.

Az adatkezelés jogszerűségének vizsgálatához a tevékenység bevezetésekor az Adatvédelmi Tisztviselő az érintett szakterületek aktív közreműködésével elvégez egy érdekmérlegelési tesztet, mely során az adatkezelés céljának szükségességét és az érintettek jogainak és szabadságainak arányos mértékű korlátozását vizsgálja és írásban megfelelően alátámasztja, összegzi.

Az érdekmérlegelési teszt során a Kar azonosítja jogos érdekét az adatkezeléshez, valamint a súlyozás ellenpontját képező érintetti érdeket és az érintett alapjogot mérlegeli. Az egymással ellentétes jogok és érdekek súlyozásának feltételét mindig az adott eset sajátos körülményeire való tekintettel vizsgálja. A Kar a mérlegelés során figyelembe veszi különösen a kezelt, illetve kezelendő adat természetét és szenzitív jellegét, nyilvánosságának mértékét, az esetlegesen bekövetkező szabálysértés súlyosságát stb.

Az érdekmérlegelési teszt részeként a szükségesség és arányosság vizsgálatát is elvégzi a Kar. A kezelhető adatok jellege és mennyisége nem haladhatja meg a jogszerű érdekek érvényesítése céljából szükséges mértéket. Az arányosság vizsgálata a célok és a megválasztott eszközök közötti kapcsolat értékelését foglalja magában. A választott eszközök a szükségesség mértékét nem haladhatják meg, azonban az eszközöknek is alkalmasnak kell lenniük a meghatározott cél elérésére.

A súlyozás elvégzése alapján a Kar megállapítja, hogy kezelhető-e a személyes adat.

A teszt eredményéről az érintettek tájékoztatást kapnak az adatkezelési tájékoztatóban, amelyben röviden ismertetésre kerül, hogy a Kar adatkezeléséhez fűződő jogos érdeke miért erősebb az érintett érdekeinél, illetve jogainál. A Kar tájékoztatja az érintetteket a hozzájárulás hiányára tekintettel alkalmazott adatvédelmi garanciákról és az adatkezelés elleni tiltakozás lehetőségeiről.

Nem írható elő az ellentétes érdekek és jogok közötti súlyozás eredménye anélkül, hogy eltérő eredményt tenne lehetővé a Kar az adott eset sajátos körülményeire tekintettel, ezért a Kar minden egyes esetben külön érdekmérlegelési tesztet végez el.

3.4.2. Érdekmérlegelési teszt elkészítésének folyamata:

3.4.2.1. A Kar a tervezett adatkezelés megkezdése előtt áttekinti, hogy a célja elérése érdekében feltétlenül szükséges-e személyes adat kezelése, megvizsgálja, hogy rendelkezésre állnak-e olyan alternatív folyamatok, adatok, amelyek alkalmazásával személyes adatok kezelése nélkül megvalósítható a tervezett cél.

3.4.2.2. A Kar az adatkezeléssel védendő jogos érdekét körültekintően és részletesen meghatározza.

3.4.2.1. A Kar meghatározza az adatkezelés lényeges körülményeit.

3.4.2.1. A Kar meghatározza, hogy az érintetteknek mik lehetnek az érdekeik az adott adatkezelés vonatkozásában (például azok a szempontok, amelyeket az érintettek felhozhatnának az adatkezeléssel szemben).

3.4.2.1. A Kar elvégzi védendő jogos érdekeinek és az érintettek vélelmezett érdekeinek, alapjogainak súlyozását és ez alapján megállapítja, hogy a személyes adat kezelhetők-e. A Kar meghatározza, hogy miért korlátozza arányosan jogos érdeke védelmében az érintetti jogokat, várakozásokat, milyen érdeksérelemmel jár a korlátozás hiánya.

3.4.2.1. A Kar meghatározza, mely garanciák biztosíthatják az adatkezelés szükségességét-arányosságát (természetesen más garanciális intézkedések is alkalmazhatók).

3.4.2.1. Az érdekmérlegelési tesztet írásban kell elkészíteni, a 6. melléklet szerinti nyomtatványon.

3.5. HATÁSVIZSGÁLAT:

Ha az adatkezelés valamely, különösen új technológiákat alkalmazó típusa valószínűsíthetően magas kockázattal jár a természetes személyek jogaira nézve az adatkezelést megelőzően hatásvizsgálatot kell végezni. Olyan egymással hasonló típusú adatkezelési műveletek, amelyek egymáshoz hasonló kockázatokat jelentenek, egyetlen adatvédelmi hatásvizsgálat (a továbbiakban: hatásvizsgálat) keretei között is értékelhetők.

A hatásvizsgálat elvégzésének szükségességéről az Adatvédelmi Tisztviselő állást foglal. A hatásvizsgálatot az érintett szakterületek készítik el az adatvédelmi tisztviselő szakmai támogatásával. A hatásvizsgálat megállapításait írásban kell rögzíteni.

Ha az Adatvédelmi Tisztviselő úgy ítéli meg, hogy az adatkezelés nem jár magas kockázattal, úgy meg kell indokolnia és dokumentumokkal igazolnia a mellőzés okait. A bevezetendő adatkezelés kizárólag a hatásvizsgálat elvégzését követően kezdhető meg.

Adatvédelmi hatásvizsgálatot a GDPR 35. cikk (3) bekezdésében, illetve a NAIH által közzétett jegyzékben (https://www.naih.hu/files/GDPR_35_4_lista_HU_mod.pdf) szereplő tevékenységek esetén kötelező elvégezni.

A fenti eseteken túl minden olyan bevezetésre kerülő – különösen az új technológiákat alkalmazó – adatkezelés esetén hatásvizsgálatot kell végezni, mely adatkezelés az ügyfélre tekintettel jelentős joghatással bír vagy az ügyfelet jelentős mértékben érinti.

A hatásvizsgálat elvégzése során Kar a NAIH honlapján közzétett szoftvert alkalmazza, a hatásvizsgálatot abban végzi el (https://naih.hu/adatvedelmi-hatasvizsgalati-szoftver.html)

A hatásvizsgálat megállapításait az adatkezelési tevékenység nyilvántartó lapjához hozzá kell csatolni és ennek megfelelően kell kialakítani az adatkezelést.

A hatásvizsgálatot legalább évente felül kell vizsgálni, szükség esetén újra el kell végezni.

3.6. ADATBIZTONSÁGI SZABÁLYOK:

3.6.1. Fizikai védelem:

A papír alapon kezelt személyes adatok biztonsága érdekében a Kar az alábbi intézkedéseket alkalmazza:

- a dokumentumokat jól zárható, száraz, tűzvédelmi és vagyonvédelmi szempontból biztosított, lehetőleg zárt helyiségben helyezi el;
- a folyamatos aktív kezelésben lévő iratokhoz csak az illetékesek férhetnek hozzá, a folyamat lezárását követően az iratokat az Iratkezelési szabályzat szerint irattárba kell helyezni;
- a Kar adatkezelést végző munkatársa a nap folyamán csak úgy hagyhatja el az olyan helyiséget, ahol adatkezelés zajlik, hogy a rá bízott adathordozókat, papír alapú adathordozókat elzárja, vagy az irodát bezárja, a kulcsot a vagyonőrök részére leadja;

- amennyiben a papíralapon kezelt személyes adatok digitalizálásra kerülnek, a digitálisan tárolt dokumentumokra irányadó biztonsági szabályokat alkalmazza a Kar, a papír alapú dokumentumokat visszaállíthatatlanul megsemmisíti, vagy az Iratkezelési szabályzatnak megfelelően irattárba helyezi.

Amennyiben a papíralapon tárolt személyes adat kezelésének célja megvalósult, úgy a Kar hivatalvezetője intézkedik a papír megsemmisítéséről. Ebben az esetben a Kar kijelöl egy munkavállalót, aki a megsemmisítésért felelős. A megsemmisítésért felelős munkavállaló a megsemmisítéssel érintett szervezeti egység bevonásával állítja össze a megsemmisítendő iratcsomagot.

A megsemmisítésen a hivatalvezető által kijelölt háromtagú megsemmisítési bizottság vesz részt. A megsemmisítésről jelen szabályzat 7. mellékletében lévő nyomtatványt kell kitölteni.

Amennyiben a személyes adatok adathordozója nem papír, hanem más fizikai eszköz, úgy a fizikai eszköz megsemmisítésére a papíralapú dokumentumokra vonatkozó megsemmisítési szabályok az irányadóak.

A Kar valamennyi adatkezelése tervezésekor, bevezetésekor speciálisan is vizsgálja az alkalmazandó fizikai védelmi intézkedéseket is.

3.6.2. Logikai védelem:

A számítógépen, illetve hálózaton tárolt személyes adatok biztonsága érdekében a Kar informatikai biztonsági szabályzatot alkot, ahol külön fejezetben rögzíti:

- a fejlesztési folyamatai során kötelezően alkalmazandó szempontrendszereit (beépített adatvédelem és információbiztonság elveinek alkalmazása),
- az informatikai eszközkezelés életciklusait,
- a jogosultság, és hozzáférésmenedzsment folyamatait,
- a mentési és archiválási rendjét,
- a naplózási rendjét,
- a külső adathordozói védelmének rendjét,
- a kötelezően alkalmazandó határvédelmi megoldásokat
- az adattárolók szerverek biztonsága (fizikai, logikai, adminisztratív) céljából alkalmazott egyéb intézkedéseit.

A Kar valamennyi adatkezelése tervezésekor, bevezetésekor speciálisan is vizsgálja az alkalmazandó logikai védelmi intézkedéseket is.

3.6.3. Álnevesítés, anonimizáció:

Az 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. Amennyiben az adat visszaállítható (az Adatkezelőnél közvetlenül rendelkezésre álló kulcs, vagy egyéb szervezetnél rendelkezésre álló kulcs használatával) anonimizált adatkezelést valósít meg Adatkezelő.

Anonimizált adatok tekintetében a feloldáshoz szükséges információt Kar logikailag elkülönülten tárolja, valamint technikai és szervezési intézkedések megtételével biztosítja, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot csak meghatározott körülmények között lehet újra kapcsolni. A fejlesztési, üzemeltetési folyamatok során minden esetben vizsgálni kell ennek a lehetőségét, és ha ez a lehetséges kockázatokkal arányos költség ellenében megvalósítható, anonimizált tárolási eljárást kell alkalmazni.

Az álnéven történő adatkezelést a Kar a statisztikai célra gyűjtendő adatok vagy a fejlesztés, tesztelés, karbantartás alatt álló rendszerek esetében a tesztadatok tekintetében végzi.

3.6.4. Beépített adatvédelem:

Fejlesztési, folyamatszervezési folyamatok során már a tervezési fázisban törekedni kell az adatvédelem elveinek érvényesülésére. Ennek érdekében át kell gondolni, hogyan valósítható meg:

- a személyes adatok kezelésének szükségességhez, adatkezelési célhoz igazodó, minimálisra csökkentése,
- a személyes adatok anonimizálása,
- a személyes adatok funkcióinak és kezelésének átláthatósága,
- a törlési kötelezettség maradéktalan teljesítése – lehetőleg az adatok álnevesítése által, így megelőzve az alkalmazásban kezelt egyéb adatok rendelkezésre állásának biztosítására vonatkozó kötelezettség sérülését,
- a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítása, integritása, rendelkezésre állása és ellenálló képessége,
- fizikai vagy műszaki incidens esetén az arra való képesség, hogy a személyes adatokhoz való hozzáférés és az adatok rendelkezésre állása kellő időben vissza állítható legyen;
- az adatkezelés biztonságának garantálására hozott technikai és szervezési intézkedések hatékonyságának rendszeres tesztelése, felmérése és értékelése rendszeres időközönként megtörténjen,
- a hozzáférési jog közvetlen gyakorlásának lehetősége kialakításra kerüljön.

A Kar és az adatfeldolgozó intézkedéseket hoz annak biztosítására, hogy az irányítása alatt eljáró, a személyes adatokhoz hozzáféréssel rendelkező természetes személyek kizárólag a Kar utasításának megfelelően kezelhessék a hivatkozott adatokat.

3.7. ADATVÉDELMI INCIDENS KEZELÉSE:

3.7.1. Adatvédelmi incidens észlelése és jelentése:

A Kar minden foglalkoztatottja – beleértve az egyéb jogviszonyban foglalkoztatott személyeket is – köteles a Karon belül történt adatvédelmi incidenst haladéktalanul jelenteni a szervezeti egysége vezetőjének, valamint az Adatvédelmi Tisztviselőnek. A bejelentésnek tartalmaznia kell a bejelentő nevét, telefonszámát, beosztását, szervezeti egységének megnevezését, valamint az incidens tárgyát, rövid leírását és azt, hogy az incidens érinti-e a Kar valamelyik informatikai rendszerét. A bejelentés megtehető szabadszöveges formában, vagy az Incidens kivizsgáló lap (8. melléklet) nyomtatványon. Telefonon tett bejelentés esetén a bejelentést követően a bejelentőnek ki kell töltenie a 8. melléklet szerinti nyomtatványt, és el kell juttatnia az Adatvédelmi Tisztviselőnek, aki a vizsgálat további szakaszaiban véglegesíti az Incidens kivizsgáló lap tartalmát.

Amennyiben az adatvédelmi incidens érinti a Kar informatikai rendszerét is, akkor a bejelentést az Informatikai Irodavezetőnek, valamint az Információbiztonsági Felelősnek is meg kell küldeni.

A bejelentés Adatvédelmi Tisztviselőhöz történő beérkezését követően az Adatvédelmi Tisztviselő haladéktalanul megkezdi az adatvédelmi incidens kivizsgálását és értékelését.

3.7.2. Adatvédelmi incidens kivizsgálása, értékelése:

Az Adatvédelmi Tisztviselő – informatikai rendszert érintő incidens esetén - az Informatikai Irodavezetővel, valamint az Információbiztonsági Felelőssel együttműködve megvizsgálja a bejelentést és amennyiben szükséges, a bejelentőtől további adatokat kér az incidensre vonatkozóan. Az Adatvédelmi Tisztviselő felhívására a bejelentő köteles megadni:

- az adatvédelmi incidens bekövetkezésének időpontját és helyét,
- az adatvédelmi incidens egyéb körülményeit,
- az adatvédelmi incidens által érintett adatok körét, mennyiségét,
- az adatvédelmi incidenssel érintett személyek körét és számát,
- az adatvédelmi incidens várható hatásait,
- az adatvédelmi incidens megelőzésére, következményeinek enyhítésére megtett intézkedések felsorolását.

A bejelentő az adatszolgáltatást a felhívást követően haladéktalanul, de legkésőbb 8 órán belül teljesíti az Adatvédelmi Tisztviselő részére.

Amennyiben az adatvédelmi incidens értékelése vizsgálatot igényel, az Adatvédelmi Tisztviselő az Informatikai Irodavezetővel, valamint az Információbiztonsági Felelőssel, valamint egyéb, a vizsgálat lefolytatásához szükséges munkatársak bevonásával lefolytatja a vizsgálatot.

A vizsgálatnak tartalmaznia kell, hogy az adatvédelmi incidens magas kockázattal jár-e az érintettek jogaira és kötelezettségeire, milyen jellegű kockázatról van szó és szükséges-e az érintettek tájékoztatása az incidensről. Amennyiben nem szükséges az érintettek tájékoztatása, a vizsgálatnak tartalmazni kell ennek indokait is.

A vizsgálat eredményeként az Adatvédelmi Tisztviselő javaslatot tesz a Hivatalvezetőnek az incidenskezeléshez szükséges intézkedések megtételére.

A javaslat alapján a megvalósítandó további intézkedésekről az adatok kezelését vagy feldolgozását végző szakterület vezetőjének véleményének figyelembevételével – informatikai rendszerben bekövetkezett adatvédelmi incidens esetében az Informatikai Irodavezető egyetértésével – a Hivatalvezető dönt.

A vizsgálatot legkésőbb a bejelentés Karhoz érkezésétől számított 72 órán belül be kell fejezni.

3.7.3. Az adatvédelmi incidens nyilvántartása:

Az adatvédelmi incidensről az Adatvédelmi Tisztviselő nyilvántartást vezet.

A nyilvántartás tartalmazza:

- az érintett személyes adatok körét,
- az adatvédelmi incidenssel érintettek körét és számát,
- az adatvédelmi incidens időpontját,
- az adatvédelmi incidens körülményeit, hatásait,
- az elhárítására megtett intézkedéseket és
- egyéb jogszabályban előírt adatokat.

Az adatvédelmi incidens nyilvántartás (9. melléklet) pontos vezetéséről, aktualizálásáról az Adatvédelmi Tisztviselő gondoskodik.

3.7.4. Az adatvédelmi incidens bejelentése a NAIH részére:

Az Adatvédelmi Tisztviselő az adatvédelmi incidenst a bekövetkezését követően haladéktalanul, de legkésőbb az incidens bekövetkezésétől számított 72 órán belül bejelenti a NAIH részére, kivéve, ha az incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Ha a bejelentés nem történik meg határidőben, az Adatvédelmi Tisztviselő köteles ennek okát igazolni a NAIH részére.

A hatósági bejelentésnek tartalmaznia kell:

- az adatvédelmi incidenssel érintett adatok körét és hozzávetőleges számát,
- az adatvédelmi incidenssel érintett személyek körét és hozzávetőleges számát,
- az adatvédelmi incidens jellegét, körülményeit,
- az Adatvédelmi Tisztviselő nevét és elérhetőségét,
- az adatvédelmi incidens valószínűsíthető következményeit és
- az adatvédelmi incidens orvoslására és enyhítésére megtett intézkedéseket.

3.7.5. Az érintettek tájékoztatása az adatvédelmi incidensről:

Ha a vizsgálat eredményeként megállapítást nyert, hogy az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságára nézve és az érintettek tájékoztatása szükséges, az Adatvédelmi Tisztviselő a Kar Hivatalvezetőjének jóváhagyásával haladéktalanul értesíti az érintetteket.

Nem kell az érintetteket tájékoztatni:

- ha a Kar olyan technikai, szervezési, védelmi intézkedéseket hajtott végre az érintett adatokra vonatkozóan, amelyek megakadályozzák az illetéktelen személyek számára való hozzáférést az adatokhoz vagy megakadályozzák az adatok értelmezhetőségét;
- ha az adatvédelmi incidens bekövetkezését követően a Kar olyan intézkedéseket tett, amelyek biztosítják, hogy a feltárt adatkezelési kockázat valószínűsíthetően nem valósul meg;
- ha a tájékoztatás aránytalan erőfeszítést tenne szükségessé. Ebben az esetben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, mely tájékoztatás elektronikus úton, vagy az Elnökség bevonásával sajtó útján is megtörténhet.

3.8. AZ ÉRINTETTEK JOGAINAK ÉRVÉNYESÍTÉSE:

A Kar személyes adatot kezel, így az érintetti jogosultságok teljesíthetőségéről köteles gondoskodni. Az erre nyitva álló teljesítési határidő a kérelem, kérés beérkezését követő legfeljebb egy hónap. Indokolt esetben a határidő hosszabbítható, az érintett indoklást is tartalmazó tájékoztatása mellett, további két hónappal.

Az érintetti joggyakorlásra írásbeli bejelentést követően van lehetőség, igénybejelentés elsősorban az adatvedelem@mbvk.hu email címen, vagy a Kar hivatalos elektronikus elérhetőségein (1. pontban jelölt elérhetőségek) tehető meg.

A Kar Adatvédelmi Tisztviselője a beérkezett kérelemről, illetve tiltakozásról köteles a beérkezéstől számított öt napon belül értesíteni az adatkezelés szempontjából feladat- és hatáskörrel rendelkező szervezeti egység vezetőjét, és részére megküldeni szakmai álláspontját a kérelem teljesíthetőségéről, a teljesítés módjáról.

A feladat- és hatáskörrel rendelkező szervezeti egység vezetője véleményegyezőség hiányában egyeztet az Adatvédelmi Tisztviselővel, majd kialakított közös álláspontjuk alapján az Adatvédelmi Tisztviselő előkészíti az érkezésétől számított legkésőbb 25 – tiltakozási jog gyakorlása esetén 15 – napon belül az Érintett részére kiadványozandó írásbeli válaszát, közérthető formában. A válasz tervezetet Adatvédelmi Tisztviselő egyeztetni köteles a Hivatalvezetővel. A Hivatalvezető jóváhagyását követően kiadmányozza a válasziratot.

3.8.1. Tájékoztatáshoz való jog (GDPR 13. és 14. cikk):

Az Adatkezelő tömör, érthető és könnyen hozzáférhető formában köteles tájékoztatni az érintettet az adatkezelés tényéről, céljáról és körülményeiről a GDPR 12-15. cikkében meghatározottak szerint. A Kar tájékoztatási kötelezettségének első sorban honlapja mbvk.hu/adatvedelem aloldalán közzétett *Általános adatkezelési tájékoztató* megnevezésű dokumentuma útján tesz eleget, mely tartalmazza valamennyi adatkezelésére vonatkozó, a GDPR-ban előírt kötelező tartalmat. A Kar az egyes adatkezelési tevékenységekről részletesebb adatkezelési tájékoztató dokumentumokat is közzé tehet, valamint az adatfelvételkor, első kapcsolatfelvételkor, vagy legkésőbb az adatok harmadik féltől való megszerzésétől számított 30 napon belül tájékoztatja az érintetteket az adatkezelési tájékoztató elérhetőségéről, vagy azt csatolja az adatfelvételi nyomtatványhoz. Kar nem tájékoztatja honlapján közzétett adatkezelési tájékoztatóin kívül más formában az érintetteket az adatkezelés lényeges körülményeiről, ha az adat megszerzését vagy közlését kifejezetten előírja az adatkezelőre alkalmazandó uniós vagy tagállami jog.

Az adatkezelési tájékoztató legalább az alábbi adatokat tartalmazza:

- tájékoztatást az Adatkezelő kilétéről, elérhetőségeiről, Adatvédelmi Tisztviselője elérhetőségeiről,
- tájékoztatást az adatkezelés céljáról, jogalapjáról, az adatkezelő vagy harmadik fél jogalapot teremtő jogos érdekeiről,
- tájékoztatást a személyes adatok címzettjeiről, illetve a címzettek kategóriáiról, EGT országon kívüli adattovábbítás esetén annak körülményeiről,
- tájékoztatást a tárolásra kitűzött időtartamról,
- tájékoztatást az érintetti joggyakorlási lehetőségekről, jogorvoslati lehetőségekről, hozzájárulás visszavonásának korlátlan lehetőségéről,
- tájékoztatást arról, hogy milyen jogi kötelezettségen alapul az adatkezelés, vagy szerződés feltétele-e, adatkezelés hiányának következményei e két esetben,

- tájékoztatást arról, hogy automatizált döntéshozatalt, profilalkotást végez e az adatkezelő, ha igen, ennek körülményeiről.

3.8.2. Hozzáférési jog (GDPR 15. cikk):

Hozzáférési joggyakorlás esetén érintett minden esetben legalább természetes személyazonosító adatainak megadására köteles, valamint rendelkeznie kell arról, hogy milyen csatornán kívánja a hozzáférési joggyakorlására kapott válasziratot kézhez venni. A Kar kizárólag a megadott adatok alapján végzi el keresését, és annak eredményéről tájékoztatja az érintettet.

Az érintett jogosult a Kartól információt kérni arra vonatkozóan, hogy vele kapcsolatban végez-e adatkezelési tevékenységet.

Ammenyiben a Kar végez az érintettel kapcsolatban adatkezelési tevékenységet, a tájékoztatási joghoz hasonlóan az érintettnek az adatkezelés során is lehetősége van a tájékoztatásban kapott információkhoz való hozzáféréshez, valamint amennyiben tagállami törvény nem rendelkezik eltérően, kérése nem lehetetlen, vagy nem érinti hátrányosan mások jogait és szabadságait, jogosult az adatkezelésben lévő adatairól egy alkalommal ingyenesen elektronikus vagy egyéb formátumú másolatot kérni.

Az Adatvédelmi tisztviselő annak érdekében, hogy az érintetti joggyakorlás teljesíthető legyen az Irodavezetőktől információt kér, hogy az általuk kezelt nyilvántartásokban az érintett által megadott adatok fellelhetőek -e valamilyen nyilvántartásban. Ha van folyamatban adatkezelési tevékenység, az Adatvédelmi Tisztviselő az Irodavezető részére továbbítja az egyedi igény alapján kialakított adatbekérő nyomtatványt, aminek kitöltését az Irodavezető 5 munkanapon belül elvégzi, és szükség esetén csatolja hozzá az adatokról készített elektronikus másolatot is.

3.8.3. Helyesbítéshez való jog (GDPR 16. cikk):

Bármely érintett kérheti az Adatkezelőtől adatainak módosítását. Erről kérelmére haladéktalanul intézkedni kell, és megadott elérhetőségére tájékoztatást kell küldeni. A valóságnak nem megfelelő adatot a Kar – amennyiben a szükséges adatok és az azokat bizonyító közokiratok rendelkezésre állnak – helyesbíti, és a GDPR. 17. cikkében meghatározott okok fennállása esetén intézkedik a kezelt személyes adat törléséről. Nem gyakorolható az érintetti jog, ha ezt jogszabály kizárja.

Helyesbítési joggyakorlás esetén az Adatvédelmi Tisztviselő a hozzáférési joggyakorlás során alkalmazott módon felméri az érintett adatkezeléseket, és megvizsgálja a teljesíthetőség feltételeit. Amennyiben az igény teljesíthető, jelzi a szakrendszert kezelő szakterület irodavezetője részére a helyesbítés végrehajthatóságát, az Irodavezető pedig 3 munkanapon belül gondoskodik annak dokumentált végrehajtásáról.

3.8.4. Törléshez való jog (GDPR 17. cikk):

A személyes adatot törölni kell,

- ha az adatkezelés jogellenes, így különösen, ha az adatkezelés az alapelvekkel ellentétes, vagy célja megszűnt, vagy az adatok további kezelése már nem szükséges az adatkezelés céljának megvalósulásához, vagy törvényben, nemzetközi szerződésben vagy az Európai Unió kötelező jogi aktusában meghatározott időtartama eltelt, vagy jogalapja megszűnt és az adatok kezelésének nincs másik jogalapja,
- az érintett az adatkezeléshez adott hozzájárulását visszavonja vagy személyes adatainak törlését kérelmezi, (kivéve a táblázatban is jelzett eseteket, valamint az adatok korlátozása esetén)
- az adatok törlését jogszabály, az Európai Unió jogi aktusa, a hatóság vagy a bíróság elrendelte.

Az adatok nem törölhetőek jogszabályban meghatározott feltételek fennállása esetén, többek között, ha azok a véleménynyilvánítás szabadságához és a tájékozódáshoz való jog gyakorlása céljából, jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez, vagy közérdekű archiválás céljából szükségesek.

Törlési kérelem esetén az Adatvédelmi Tisztviselő a hozzáférési joggyakorlás során alkalmazott módon felméri a vonatkozó adatkezeléseket, és megvizsgálja a teljesíthetőség feltételeit. Amennyiben az igény teljesíthető, jelzi a szakrendszert kezelő szakterület Irodavezetője részére, hogy a törlést teljesíteni kell. Az Irodavezető 3 munkanapon belül gondoskodik annak dokumentált végrehajtásáról.

3.8.5. Az adatkezelés korlátozásához való jog (GDPR 18. cikk):

Az érintett jogosult arra, hogy kérésére az adatkezelő korlátozza az adatkezelést, amennyiben az alábbi feltételek valamelyike áll fenn:

- az érintett vitatja a személyes adatok pontosságát,
- az adatkezelés jogellenes és az érintett ellenzi az adatok törlését, ehelyett kéri azok felhasználásának korlátozását,
- a Karnak már nincs szüksége a személyes adatokra az adatkezelés céljából, azonban az érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez,
- az érintett tiltakozik az adatkezelés ellen, ez esetben a korlátozás arra az időtartamra vonatkozik, amíg megállapításra nem kerül, hogy Kar jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben.

A korlátozott adatokkal csak az érintett hozzájárulásával, jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez, vagy más természetes vagy jogi személy jogainak védelme érdekében, vagy az Unió, illetve valamely tagállam által meghatározott fontos közérdekéből végezhető tároláson kívül egyéb művelet.

Korlátozás kérés esetén Adatvédelmi Tisztviselő a hozzáférési joggyakorlás során alkalmazott módon felméri az érintett adatkezeléseket, és megvizsgálja a teljesíthetőség feltételeit. Amennyiben az igény teljesíthető, jelzi a szakrendszert kezelő szakterület irodavezetője részére, hogy az adattal az ismételt értesítésig a tároláson kívül egyéb művelet nem végezhető. Abban az esetben, ha a korlátozás időtartama vélhetően meghaladja a megőrzésre kijelölt időt, külön figyelmet kell fordítani arra, hogy az adatokat az azt kezelő rendszer ne törölje vagy anonimizálja, papír alapú adatkezelés esetén az adathordozó selejtezésére ne kerüljön sor.

Irodavezető haladéktalanul, legkésőbb 1 munkanapon belül gondoskodik az adatkezelés korlátozásának dokumentált végrehajtásáról.

3.8.6. Adathordozhatósághoz való jog (GDPR 20. cikk):

Ha az adatkezelés az érintett hozzájárulásán alapul, vagy szerződéskötéshez, vagy annak teljesítéséhez szükséges, és az adatkezelés automatizált módon történik, az érintett jogosult arra, hogy a rá vonatkozó, általa az Adatkezelő rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formában megkapja, továbbá jogosult arra, hogy kérésére adatkezelő ezeket az adatokat egy másik adatkezelőnek továbbítsa.

Adathordozási kérés esetén az Adatvédelmi Tisztviselő a hozzáférési joggyakorlás során alkalmazott módon felméri az érintett adatkezeléseket, és megvizsgálja a teljesíthetőség feltételeit. Amennyiben az igény teljesíthető, jelzi az Informatikai Irodavezető részére a másolat elkészítésének igényét, akik 15 munkanapon belül elkészítik az elektronikus másolatot.

3.8.7. Tiltakozáshoz való jog (GDPR 21. cikk):

Az érintett tiltakozhat személyes adatának kezelése ellen,

- ha a személyes adatok kezelése vagy továbbítása közérdekű feladatellátáshoz kapcsolódó, vagy közhatalmi jogosultságok érvényesítéséhez szükséges jogalapon vagy a Kar, adatátvevő vagy harmadik személy jogos érdekének érvényesítéséhez szükséges jogalapon történik;
- ha a személyes adat felhasználása vagy továbbítása közvetlen üzletszerzés, közvélemény-kutatás vagy tudományos kutatás céljára történik; valamint
- törvényben meghatározott egyéb esetben.

Adatvédelmi Tisztviselő a tiltakozást a kérelem benyújtásától számított legrövidebb időn belül, de legfeljebb 15 napon belül megvizsgálja, annak megalapozottsága kérdésében döntést hoz, és döntéséről a kérelmezőt írásban tájékoztatja. Ha az Adatvédelmi Tisztviselő az érintett tiltakozásának megalapozottságát megállapítja, haladéktalanul értesíti az illetékes szakterület Irodavezetőjét, hogy intézkedjen az adott érintett vonatkozásában az adatkezelés - beleértve a további adatfelvételt és adattovábbítást is – megszüntetéséről, a kezelt adatok korlátozásáról, továbbá értesítse az összes olyan címzettet, akinek részére a tiltakozással érintett személyes adatot korábban továbbította, és -e címzettek

dokumentáltan gondoskodjanak arról, hogy az Adatvédelmi Tisztviselő által meghatározott intézkedések végrehajtásra kerüljenek.

4. ZÁRÓ RENDELKEZÉSEK:

Jelen szabályzat hatálya alá tartozó személyeknek a szabályzat rendelkezéseit meg kell ismerniük és annak tényét az aláíróíven igazolniuk kell.

A jelen szabályzat 2026. május 21. napján lép hatályba.

Módosítás esetén az Adatkezelő jelen szabályzat közzétételével egyező módon tájékoztatja az érintetteket (közzététel a honlapon, intranet) a módosított rendelkezésekről.

Jelen szabályzat rendelkezéseit alkalmazni kell a hatálybalépésekor már folyamatban lévő adatkezelési tevékenységekre, érintetti joggyakorlásokra és incidenskezelési folyamatra is.

Budapest, 2026. május 21.

Magyar Bírósági Végrehajtói Kar
Hivatal Budapest
I.

.....

dr. Takács Katalin

hivatalvezető

MELLÉKLETEK

1. melléklet

Szerződésekben használandó adatvédelmi, titoktartási, kapcsolattartási klauzulák

1. ADATVÉDELEM

1. [kitöltendő] jelen szerződésben személyes adatok kezelésével is járó szakértői feladatok ellátására vállalt kötelezettséget, amely feladatok végrehajtása során adatfeldolgozóként adatkezelési tevékenységet végez jelen [kitöltendő] részére a Szerződés [kitöltendő]. mellékletében meghatározott feltételeknek megfelelően. Az adatfeldolgozói megállapodás a Szerződés elválaszthatatlan része.

2. TITOKTARTÁS

Jelen [kitöltendő] pontban foglalt titoktartási rendelkezések alkalmazását jogszabály kizárhatja, korlátozhatja. A Szerződés megszűnése nem érinti a Felek titoktartási kötelezettségét. Tekintettel arra, hogy [kitöltendő] közfeladatot ellátó szerv, a Szerződésben rögzített szolgáltatás közfeladat ellátáshoz kapcsolódik, Felek ilyen korlátozó rendelkezésként ismerik el kifejezetten az információs önrendelkezési jogról és információszabadságról szóló 2011. évi CXII. törvény 3. § 5. pontját, 26. § (1) bekezdését és 27. §- át, kiemelten a 27. § (3) bekezdését. Felek vállalják, hogy a másik felet is érintő közérdekű adatigénylést teljesítését megelőzően kölcsönösen értesítik egymást a beérkezett adatigénylésről, a tervezett válasz tartalmáról.

A Szerződés aláírásával Felek feltétlen és visszavonhatatlan kötelezettséget vállalnak arra, hogy a Szerződés végrehajtása során tudomásukra jutott minden adatot, információt időbeli korlátozás nélkül, a 2018. évi LIV. törvénynek megfelelően, külön minősítési eljárás nélkül is üzleti titokként kezelnek. Felek az átadott mindennemű információt kizárólag a Szerződés keretei között használhatják, kizárólag azoknak a szintén titoktartási kötelezettség hatálya alatt álló személyeknek hozhatják tudomására, akiknek azt a Szerződésben meghatározott célok elérése érdekében tudniuk kell. Felek az információt ugyanolyan gondossággal kötelesek kezelni, mint amellyel a hasonló információk titkosságát és bizalmas jellegét saját szervezetükön belül védik. Az üzleti titok az átadó fél tulajdonában marad és a fogadó félnek történő átadás (tudomásra hozás) csak korlátozott engedélyt ad Feleknek, vagy bármely velük a Szerződéssel kapcsolatban jogviszonyban álló harmadik személynek a fenti információ felhasználására.

Felek rögzítik, hogy a titoktartási kötelezettség megsértését súlyos szerződésszegésnek tekintik. Ilyen esetekben Felek azonnali hatállyal jogosultak a Szerződés megszüntetésére.

3. KAPCSOLATTARTÓ SZEMÉLYEK

A Felek a Szerződés teljesítéséhez szükséges kapcsolattartás céljából a szerződéskötéssel egyidejűleg kötelesek az illetékes képviselőiket kijelölni a [kitöltendő] mellékletként csatolt nyilatkozat kitöltésével és érintetti nyilatkozatok beszerzésével. A Felek kötelesek a saját Kapcsolattartóik személyes adatában bekövetkezett változásról a másik Felet haladéktalanul tájékoztatni, új kapcsolattartó kijelölésekor a nyilatkozatot az érintettel ismertetni, kitöltve a másik Fél rendelkezésére bocsátani. A Felek kötelesek a másik fél Kapcsolattartójának személyes adatát véglegesen és helyreállíthatatlanul törölni/megsemmisíteni, amennyiben az azok kezelésére vonatkozó jogalap és/vagy az adatkezelési cél megszűnik.

A Felek rögzítik, hogy egymás között minden nyilatkozatot elektronikus úton (biztonságos kézbesítési csatorna használatával), írásban, szükség szerint tértivevényes levélben, vagy e-mailben kell megküldeni, amely akkor tekinthető jogszerűen kézbesítették, ha azt a képviseletre jogosult vagy a kapcsolattartó személyek részére az MBVK rövid nevű hivatali kapura, a mellékletben megjelölt email címre, vagy postai címre kézbesítették. Az értesítés akkor válik hatályossá, amikor azt a címzett igazoltan átvette. Az e-mail útján történő kézbesítés esetén a nyilatkozat vagy értesítés a kiküldést követő ötödik munkanapon kézbesítettnek tekintendő.

Kapcsolattartók megjelölése és adatkezelési tájékoztató

[kitöltendő] részéről

Értesítések fogadására és küldésére jogosult személy(ek)

- **név:** **[kitöltendő]**
- email cím: [kitöltendő]
- telefonszám: [kitöltendő]
- betöltött pozíció: [kitöltendő]

Megértettem, hogy jelen [kitöltendő] szerződés kapcsán [kitöltendő] szakértőként, a Felek között létrejött jognyilatkozatok és egyéb dokumentumok, utasítások érvényességének szükség szerinti igazolásához, az ezzel kapcsolatos esetleges jogérvényesítés megvalósíthatóságához, a kapcsolatfelvételhez és kapcsolattartáshoz, továbbá a szerződéssel kapcsolatos általános adminisztrációk elvégzéséhez személyes adataim [kitöltendő], mint Adatkezelő adatkezelésébe kerülnek.

[kitöltendő] jogaimat ismertette, Adatkezelő adatkezeléssel kapcsolatos tájékoztatóját [hivatkozás annak elérhetőségére, vagy adatkezelés lényeges körülményeinek ismertetése] megismertem, a benne foglaltakat megértettem, és elfogadom.

Kelt: Budapest, [kitöltendő]

_____

XY

[kitöltendő] részéről

Értesítés fogadására és küldésére jogosult személyek

- **név:** **[kitöltendő]**
- email cím: [kitöltendő]
- telefonszám: [kitöltendő]
- betöltött pozíció: [kitöltendő]

Megértettem, hogy jelen [kitöltendő] szerződés kapcsán kapcsolattartóként, a Felek között létrejött jognyilatkozatok és egyéb dokumentumok, utasítások érvényességének szükség szerinti igazolásához, az ezzel kapcsolatos esetleges jogérvényesítés megvalósíthatóságához, a kapcsolatfelvételhez és kapcsolattartáshoz, továbbá a szerződéssel kapcsolatos általános adminisztrációk elvégzéséhez személyes adataim [kitöltendő], mint Adatkezelő adatkezelésébe kerülnek a felelősségre vonhatóság elévülésének idejéig, de legfeljebb a szerződés teljesülését követő 5 évig. Adataim nem kerülnek továbbításra harmadik fél részére.
[kitöltendő] tájékoztatott, hogy jogaimmal kapcsolatos bővebb információt az alábbi elérhetőségen találok: mbvk.hu/adatvedelem/4 weboldalon tájékozódhatok.
Adatkezelő adatkezeléssel kapcsolatos tájékoztatóját megismertem, a benne foglaltakat megértettem, és elfogadom.

Kelt: Budapest, [kitöltendő]

2. melléklet

Adatfeldolgozói szerződés minta

Adatfeldolgozói megállapodás

mely létrejött

[Kitöltendő] (székhely:[kitöltendő]; adószám:[kitöltendő];képviseli:[kitöltendő]) mint Megbízó és Adatkezelő (továbbiakban: [kitöltendő] vagy Adatkezelő), és

[Kitöltendő] (székhely: [kitöltendő], adószám: [kitöltendő], mint megbízó, képviseli: [kitöltendő]) mint [kitöltendő] és Adatfeldolgozó (továbbiakban: [kitöltendő] vagy Adatfeldolgozó),

együttesen Felek között az alábbiakban meghatározott helyen, időben és tartalommal.

1. Adatkezelési tevékenység leírása, érintett adatok köre

1.1. [Szerződéses tevékenység leírása]

1.2. Adatfeldolgozó feladata:

- [kitöltendő]
- [kitöltendő]
- [kitöltendő]

2. A Felek jogai és kötelezettségei

2.1. Adatfeldolgozó az 1. pontban meghatározott adatfeldolgozási tevékenység ellátására vállal kötelezettséget. Az adatfeldolgozási tevékenység elvégzéséért külön díjazás Adatfeldolgozót nem illeti meg.

2.2. Adatfeldolgozó az adatokkal kapcsolatos érdemi döntést nem hozhat, kizárólag az Adatkezelő által a jelen megállapodásban meghatározottak szerinti feladatok elvégzésére jogosult és a tudomására jutott személyes adatokat kizárólag az Adatkezelő írásbeli utasításai szerint kezelheti. Adatfeldolgozó a feladatellátása során az Adatkezelő nevében és annak megbízásából, továbbá rendelkezésének megfelelően (utasítási jog) végzi a tevékenységét. Adatkezelő nevében utasítási jogkörrel rendelkező személy a Hivatalvezető, az Adatvédelmi Tisztviselő, valamint a szerződésben kapcsolattartóként megjelölt személy. Írásbeli utasítást az Adatfeldolgozó 1. pontba megjelölt elérhetőségére köteles címezni Adatkezelő.

2.3. Feladata ellátása céljából Adatkezelő [adatmegosztás módja kitöltendő] megosztja Adatfeldolgozóval az üzleti titkot és személyes adatot is tartalmazó állományt. Az átadott adatokat Adatfeldolgozó nem jogosult továbbítani, megosztani további címzettekkel, [ide nem értve az 1.2 pontban meghatározott célból igénybe veendő további adatfeldolgozót és adattovábbítást], adatok bizalmasságának megőrzéséért jelen megállapodás hatályától független, időben korlátlan titoktartási kötelezettség terheli. Az adatokkal kizárólag az 1.2 pontban meghatározott műveletek elvégzésére jogosult.

2.4. Adatfeldolgozó tudomásul veszi, hogy amennyiben az Európai Unió 2016/679 rendeletének (a továbbiakban: GDPR) rendelkezéseit sértve maga határozza meg az adatkezelés céljait és eszközeit, akkor őt az adott adatkezelés tekintetében adatkezelőnek kell tekinteni, és teljeskörűen viselni köteles az adatkezelői minőséggel kapcsolatos jogokat és kötelezettségeket, jelen megállapodás megszegésének jogi következményeit.

2.5. Adatkezelő kizárólag a mellékletben megjelölt további adatfeldolgozó igénybevételére jogosítja az Adatfeldolgozót. Adatfeldolgozó részére az 1.2 pontban meghatározott adatkörben, és adatkezelési célból, adatkezelési műveletek elvégzésére továbbítható adat.

2.6. Adatfeldolgozó köteles a személyes adatokat érintő bármely incidensről (különösen a kezelt személyes adatokhoz való illetéktelen hozzáférésről, a jogosulatlan megváltoztatásról vagy a hozzáférhetetlenné válásról) a tudomásszerzését követően haladéktalanul (legkésőbb 8 órán belül) írásban tájékoztatni (adatvédelmi kérdésekben alkalmazott elérhetőségére küldött elektronikus levél formájában) Adatkezelőt annak érdekében, hogy a GDPR-ban meghatározott – incidensek kezelésével járó – kötelezettségeit teljesíteni tudja, továbbá köteles Adatkezelőt segíteni az esetleges adatvédelmi vizsgálat lefolytatásával összefüggő feladatai ellátásában.

2.7. Az adatfeldolgozási tevékenység során Adatfeldolgozó megfelelő technikai és szervezési intézkedések útján garantálja a kezelt személyes adatok biztonságát, azok bizalmas jellegének biztosítását, valamint integritását és rendelkezésre állását. Adatfeldolgozó különösen az alábbi technikai és szervezési intézkedéseket hajtja végre annak érdekében, hogy a megfelelő szintű adatbiztonságot garantálja:

- biztosítja, hogy a nevében eljáró személyek titoktartási kötelezettség hatálya alatt álljanak;
- [kitöltendő]
- [kitöltendő]

- [kitöltendő]

2.8. Adatkezelő jogosult ellenőrizni Adatfeldolgozónál a szerződés szerinti tevékenység végrehajtását és a megtett védelmi intézkedéseket a hatékonyság és biztonság érdekében.

2.9. Adatfeldolgozó az Adatkezelő megkeresésére a hatásvizsgálat elkészítésében vagy módosításában is adatszolgáltatási támogatást biztosít az Adatkezelőnek.

3. Érintetti joggyakorlás

3.1. Az adatkezelés jellegének figyelembevételével az érintetti joggyakorlások esetén kizárólag Adatkezelő jogosult az érintettek kérelmének megválaszolására, ehhez szükség szerint kérheti Adatfeldolgozó közreműködését, aki a kérés érkeztetését követő 5 munkanapon belül Adatkezelő rendelkezésére áll.

4. Kártérítési felelősség meghatározása

4.1. Adatfeldolgozó kijelenti, hogy amennyiben a jelen szerződésben, továbbá a GDPR-ban, valamint a vonatkozó ágazati jogszabályokban foglalt, adatvédelemmel összefüggő bármely kötelezettségét neki felróható módon megszegi, az ebből eredő vagyoni, illetve nem vagyoni károkat köteles teljes mértékben megtéríteni, beleértve az Adatfeldolgozó magatartásából eredően az Adatkezelő terhére kirótt adatvédelmi bírságokat is.

4.2. Felek kötelezettséget vállalnak arra, hogy minden olyan körülményről tájékoztatják egymást, amely a szerződés teljesítését, illetve a másik Fél jogos érdekét érinti. A bejelentési kötelezettség elmulasztásából eredő károkért a mulasztó Fél teljes kárfelelősséggel tartozik.

5. Adatfeldolgozói megállapodás hatálya, módosítása, megszűnése

5.1. Jelen megállapodás a Felel általi aláírással lép hatályba, és a szerződésben meghatározott tevékenység elvégzéséig tartó ideig jogosítja és kötelezi a Feleket a benne foglaltakra. Jelen szerződés megszűnésével egyidejűleg Adatfeldolgozó minden még birtokában lévő személyes adatot és készített másolatot az Adatkezelő rendelkezésének megfelelően töröl úgy, hogy azok fizikai és logikai helyreállítása a továbbiakban nem lehetséges.

A jelen megállapodásban nem szabályozott kérdésekben a GDPR, a Ptk., továbbá a vonatkozó ágazati jogszabályok rendelkezései irányadók.

Jelen szerződést a Felek, mint akaratukkal mindenben megegyezőt helyben hagyólag írták alá.

Budapest, [kitöltendő]

[kitöltendő]
képviseli: [kitöltendő]
Adatkezelő

[kitöltendő]
képviseli: [kitöltendő]
Adatfeldolgozó

3. melléklet

Titoktartási nyilatkozat minta

TITOKTARTÁSI NYILATKOZAT

Alulírott név: [kitöltendő] születési idő, hely: [kitöltendő], a [kitöltendő] (székhely: [kitöltendő]; adószám: [kitöltendő]) munkavállalójaként/ egyéb közreműködőjeként nyilatkozom az alábbiakról:

Jelen nyilatkozat tétellel kötelezem magam, hogy az előttem [jogviszony specifikusan kitöltendő] a Magyar Bírósági Végrehajtói Kar (továbbiakban, mint „Kar") által feltárt, és a jövőben feltárandó információkat, így különösen üzleti titkokat, [jogviszony specifikusan kitöltendő], és bármilyen egyéb információt az üzleti titokról szóló 2018. évi LIV. törvényben foglaltaknak megfelelően, üzleti titokként kezelek, a tevékenységem során a hatályos jogszabályoknak, a Kar utasításainak megfelelően járok el.

Tudomásul veszem, hogy amennyiben az információt a hatályos jogszabályoknak nem megfelelő módon (különösen ideértve üzleti titokra vonatkozó titoktartási kötelezettség megszegésével), a Kar utasításaival nem egyező módon, vagy Kar Szabályzatában foglaltakat nem figyelembe véve kezelem, teljeskörűen terhel a magatartásomból eredő kárfelelősség.

Tudomásul veszem továbbá, hogy titoktartási kötelezettségem alól - az engedélyben meghatározott információk erejéig - csak jogszabály rendelkezése alapján, vagy a Magyar Bírósági Végrehajtói Kar írásbeli engedélyével mentesülhetek.

Tudomásul veszem továbbá, hogy jelen nyilatkozatban szabályozott titoktartási kötelezettség időbeli hatálya korlátlan. Megértettem, hogy a jelen nyilatkozatban foglalt kötelezettség megszegése esetén szakmai, polgári jogi és – szándékosság esetén – büntetőjogi felelősséggel tartozom.

Budapest, [kitöltendő]

.....

Aláírás

A jelen nyilatkozat aláírásával tudomásul veszem és megértettem, hogy a fent megadott személyes adataimat a Kar, mint Adatkezelő, a vonatkozó adatvédelmi szabályoknak megfelelő az Adatkezelő magántulajdonhoz és üzleti titkainak, nyilvántartásaiban kezelt személyes adatok védelméhez fűződő jogos érdeke alapján kezeli, és megőrzi a felelősségre vonhatóság elévülésének idejéig. Megértettem, hogy adataim továbbításra nem kerülnek, jogaimmal kapcsolatos bővebb tájékoztatást az alábbi elérhetőségen találok: mbvk.hu/adatvedelem/5

Oktatási rend

Oktatások lebonyolításának hónapja és tervezett tematika

Jogi Iroda

Oktatás tervezett hónapja: tárgyév november

Tervezett tematika:

- Érintetti jogok, joggyakorlás felismerése
- Incidens, incidenskezelés
- Egyes adatkezelési tevékenységekkel kapcsolatos speciális ismeretek:
  - Szerződésekkel kapcsolatos adatkezelések,
  - Ügyfél megkeresésekkel kapcsolatos adatkezelések,
  - Közhiteles ügynyilvántartással kapcsolatos adatkezelések,
  - Ügykiosztó rendszerrel kapcsolatos adatkezelések,
  - Iroda nyilvántartással kapcsolatos adatkezelések,
  - Fegyelmi eljárások kezdeményezése, folyamatban lévő fegyelmi eljárások nyilvántartása,
  - Felfüggesztések,
  - Iroda átadás,
  - Titoktartás alóli felmentések,
  - Peres ügyek,
  - Szakmai gyakorlat igazolása,
  - Elektronikus árverési rendszer,
  - VIEKR,
  - Ügykiosztás,
  - Iktatás,
  - Névjegyzék,
  - Közhiteles ügynyilvántartás,
  - Végrehajtói adatszolgáltatási platform,
  - Végrehajtói kézbesítések.

Oktatás tervezett hónapja: tárgyév január

Tervezett tematika:

- Érintetti jogok, joggyakorlás felismerése
- Incidens, incidenskezelés
- Egyes adatkezelési tevékenységekkel kapcsolatos speciális ismeretek:
  - Végrehajtói ügyfélszolgálat,
  - Végrehajtói, végrehajtó-helyettesi, végrehajtójelölti névjegyzék,
  - Oktatások,
  - Rendezvények, utazások,
  - Elnökségi ülések, Taggyűlés,
  - Iratkezelés,
  - Szárazbélyegző, biztonsági papír, jelvény nyilvántartás,
  - Jogakadémia jegyzőkönyvek,
  - Kézbesítési vizsgák, meghallgatások,
  - Toborzásokkal kapcsolatos adatkezelések.

Ellenőrzési és Fegyelmi Iroda

Oktatás tervezett hónapja: tárgyév december

Tervezett tematika:

- Jogszerű adatkezelés az ellenőrzés során- mit lehet, és mit nem lehet?
- Jogszerű adatkezelés a végrehajtói irodákban
- Ellenőrzött adatállományok adatbiztonsága és adatállományok megőrzési ideje
- Egyes adatkezelési tevékenységekkel kapcsolatos speciális ismeretek:
  - Végrehajtói irodák ellenőrzése.

Gazdasági és Pénzügyi Iroda

Oktatás tervezett hónapja: tárgyév február

Tervezett tematika:

- Érintetti jogok, joggyakorlás felismerése
- Incidens, incidenskezelés

- Egyes adatkezelési tevékenységekkel kapcsolatos speciális ismeretek:
  - Munkáltatói adatkezelések,
  - Általános költségátalánnyal kapcsolatos adatkezelések,
  - Állam által megelőlegezett költségekkel kapcsolatos adatkezelések,
  - Számlák és bizonylatok, pénz- és értékkezelés, utalványozás, pénzügyi ellenjegyzés,
  - Gazdálkodási rendszer- partnerek nyilvántartása,
  - Tagdíj befizetések,
  - Fizetési meghagyások kézbesítésének költségei,
  - Leltározások,
  - Beszerzések,
  - Mobilflotta, telefonhasználat ellenőrzése,
  - Útnyilvántartás, gépjármű használat engedélyezése, gépjárművekkel kapcsolatos baleseti jegyzőkönyvekhez kapcsolódó adatkezelés.

Ügyfélszolgálati és Panasz Iroda

Oktatás tervezett hónapja: tárgyév március

Tervezett tematika:

- Érintetti jogok, joggyakorlás felismerése
- Incidens, incidenskezelés
- Egyes adatkezelési tevékenységekkel kapcsolatos speciális ismeretek:
  - Telefonos és honlapon keresztül indított kapcsolatfelvétellel kapcsolatos adatkezelés,
  - Panaszügyintézéssel kapcsolatos adatkezelés,
  - Ügykiosztás,
  - Iktatás, Tanúsítványokkal kapcsolatos tájékoztatás,
  - Ügyfél megkeresésekkel kapcsolatos tájékoztatás,
  - Végrehajtókkal és végrehajtói irodákkal kapcsolatos tájékoztatás,
  - Informatikai helpdesk,
  - VIEKR,
  - EÁR.

Informatikai Iroda

Oktatás tervezett hónapja: tárgyév április

Tervezett tematika:

- Incidens, incidenskezelés,
- Adatbiztonsági követelmények,
- Egyes adatkezelési tevékenységekkel kapcsolatos speciális ismeretek:
  - Elektronikus árverési rendszer,
  - VIEKR,
  - Ügykiosztás,
  - Levelező rendszer,
  - Végrehajtói, végrehajtó-helyettesi levelezés
  - Iktatás,
  - Névjegyzék,
  - Közhiteles ügynyilvántartás,
  - Végrehajtói adatszolgáltatási platform,
  - Tanúsítvány nyilvántartás,
  - Jogosultságok,
  - Eszközkiadás, eszköz nyilvántartás,
  - WIFI hozzáférések,
  - Informatikai helpdesk,
  - Honlap,
  - Adatmegsemmisítések,
  - Biztonsági mentés,
  - Archiválás.

5. melléklet

Adatkezelési tevékenység nyilvántartó lap

Adatkezelési tevékenység nyilvántartó lap - bevezetés

[Adatkezelési tevékenység sorszáma]	**[Adatkezelés megnevezése]**	
Adatkezelésért felelős szervezeti egység:		
Bevezetés oka:		
Bevezetés dátuma:		
Adatkezelés tervezett folyamata:		
Érintettek köre:		
Kezelendő adatok köre, adatkezelési cél adatkörönként		
Adatkezelés jogalapja:		
Jogalap indoklása:		
Adatok forrása		
Hogyan történik az adatok felvétele, tárolása?		
Érintett szakrendszerek		
Lehetséges kockázatok		
Alkalmazott adatbiztonsági intézkedések leírása		
Adattovábbítás történik? Ha igen, hova?		
EGT országon kívüli adattovábbítás esetén megfelelősségi határozat, vagy megfelelő garancia		
Adatfeldolgozó igénybevétele		
Adatfeldolgozói megállapodás		
Adatkezelésről tájékoztatás módja		
Adatkezelés tervezett időtartama		

Adatkezelési tevékenység nyilvántartó lap - módosítás

[Adatkezelési tevékenység sorszáma]	**[Adatkezelés megnevezése]**	
Módosítás sorszáma		
Adatkezelésért felelős szervezeti egység:		
Módosítás oka:		
Módosítás dátuma:		
Adatkezelés tervezett folyamata a módosítást követően		
Érintettek köre a módosítást követően:		
Kezelendő adatok köre, adatkezelési cél adatkörönként- a módosítást követően:		
Adatkezelés jogalapja a módosítást követően:		
Jogalap indoklása a módosítást követően:		
Adatok forrása a módosítást követően:		
Hogyan történik az adatok felvétele, tárolása a módosítást követően?		
Érintett szakrendszerek a módosítást követően:		
Lehetséges kockázatok		
Alkalmazott adatbiztonsági intézkedések leírása a módosítást követően		
Adattovábbítás történik? Ha igen, hova?		
EGT országon kívüli adattovábbítás esetén megfelelősségi határozat, vagy megfelelő garancia		
Adatfeldolgozó igénybevétele a módosítást követően		
Adatfeldolgozói megállapodás a módosítást követően		
Adatkezelésről tájékoztatás módja a módosítást követően		
Adatkezelés tervezett időtartama		

Adatkezelési tevékenység nyilvántartó lap – adatkezelés kivezetése

[Adatkezelési tevékenység sorszáma]	**[Adatkezelés megnevezése]**
Kivezetésért felelős szervezeti egység:	
Kivezetés oka:	
Kivezetés dátuma:	
Adatkezelés kivezetését követően archívként megőrzendő?	
Érintettek köre	
Kivezetendő adatok köre	
Hogyan történik az archív adatok tárolása?	
Érintett szakrendszer	
Lehetséges kockázat	
Alkalmazott adatbiztonsági intézkedések leírása	
Adattovábbítás történik? Ha igen, hova?	
Adatfeldolgozó igénybevétele a módosítást követően	
Adatfeldolgozói megállapodás	
Adatkezelés kivezetéséről hogyan történik az Érintettek tájékoztatása	

6. melléklet

Érdekmérlegelési teszt minta

[Tervezett adatkezelés megnevezése]	
Adatkezelés tervezett célja	
Adatkezelés tervezett időtartama	
Kezelendő adatok tervezett köre	
Adatfeldolgozás tervezett folyamata	
Adatkezelés szükséges?	
Létezik alternatív mód az adatkezelés cél elérésére?	
1. Adatkezelő jogszerű érdekeinek értékelése	
Védendő alapvető jogok felsorolása (EJEE, Alapjogi Charta, Alaptörvény)	
Közérdek, közösségi érdek	
Egyéb jogos érdek	
Az érdekek jogszerűségének jogi és kulturális /társadalmi elismerése	
Adatkörök korlátozása	
Adattárolás időtartamának korlátozása	
Anonimizálási technikák	
Aggregált adatok	
Tiltakozási jog biztosítása	
Törlési kérés mérlegelés nélküli teljesítése	
Egyéb adatbiztonsági intézkedés	
Egyéb szervezési intézkedés	
2. Érintettre gyakorolt hatás	
Adatkezelés lehetséges következményei	
Kockázat bekövetkezésének lehetősége	
Kockázat súlyossága	
Érintettek potenciális száma	
Felek státusza	
Érintett ésszerű elvárása	
3. Érdekek egyensúlya megállapítható?	
Igen	Nem
4. Amennyiben nem, további biztosítékok meghatározása	
Adatkörök korlátozása	
Adattárolás időtartamának korlátozása	
Anonimizálási technikák	
Aggregált adatok	
Tiltakozási jog biztosítása	
Törlési kérés mérlegelés nélküli teljesítése	
Egyéb adatbiztonsági intézkedés	
Egyéb szervezési intézkedés	
5. Érdekek egyensúlya megállapítható a biztosítékok alkalmazását követően?	
Igen	Nem

7. melléklet

Adatmegsemmisítési jegyzőkönyv minta

Jegyzőkönyv irat/adatmegsemmisítésről

Irat/Adatmegsemmisítési bizottság tagjai

(1) Munkavállaló neve: .....
Születési hely, idő: .....
Munkakör: .....

(2) Munkavállaló neve: .....
Születési hely, idő: .....
Munkakör: .....

(3) Munkavállaló neve: .....
Születési hely, idő: .....
Munkakör: DPO

A megsemmisítés tárgya, adathordozó típusa és száma:

[kitöltendő]

A megsemmisítés módszere

[kitöltendő]

A megsemmisítés oka

[kitöltendő]

Adatmegsemmisítés helye és ideje

[kitöltendő]

[kitöltendő]

Az adatok megsemmisítését jóváhagyom:

Hivatalvezető

Aláírásommal igazolom, hogy az adatok törlése a jegyzőkönyvben rögzítetteknek megfelelően megtörtént.

Kelt: Budapest, [kitöltendő]

_____ _____

Név Név

_____

Név

8. melléklet

Incidens kivizsgáló lap
Jegyzőkönyv lehetséges adatvédelmi incidens kivizsgálásáról

Jelen jegyzőkönyv a [kitöltendő éééé.hh.nn-én óó:pp-kor] történt az [kitöltendő] rendszerrel kapcsolatos [kitöltendő üzemzavar/bejelentés] [kitöltendő] által észlelt lehetséges incidens (továbbiakban: lehetséges incidens vagy esemény) kivizsgálásával kapcsolatos részletes információkat tartalmazza.

Adatkezelő:

Cím:

1. ESEMÉNY KIVIZSGÁLÁSA ELŐTT ISMERT KÖRÜLMÉNYEK

Vizsgálat tárgya:

Esemény rövid leírása:

Eseményt észlelő személy:

Az esemény felfedezésének helye:

Az esemény felfedezésének ideje:

Egyéb észleléssel kapcsolatos körülmény:

A lehetséges incidens bekövetkezésének helye:

A lehetséges incidens bekövetkezésének ideje

Adatkezelő mikor értesült az eseményről?

2. VIZSGÁLAT SORÁN FELTÁRTAK

Vizsgálat helye és ideje

Esemény melyik adatkezelési tevékenységhez kapcsolódik?

Esemény kapcsolódik informatikai rendszerhez? Ha igen, melyik rendszerhez?

Az esemény kapcsán biztosan érintett / részt vevő személyek (név, titulus, szerep az eseményben (pl rendszergazda, munkavállaló, bejelentő, észlelő stb.)

Esemény érint személyes adatokat?

Esemény érinti személyes adatok különösen védett kategóriáját (9. cikk (1) bekezdés)

Rendelkezésre álló és vizsgált bizonyítékok

Vizsgálat tapasztalata

Az esemény lehetséges bekövetkezésének körülményei

Megállapítható személyes adatok véletlen vagy jogellenes **megsemmisítése**?

Megállapítható személyes adatok véletlen vagy jogellenes **elvesztése**?
Megállapítható személyes adatok véletlen vagy jogellenes **megváltoztatása**?
Megállapítható személyes adatok véletlen vagy jogellenes **közlése?**
Megállapítható személyes adatok véletlen vagy jogellenes **hozzáférés?**

amennyiben igen/nem

ADATVÉDELMI INCIDENS TÖRTÉNT?

további szakaszok kitöltése kizárólag akkor szükséges, ha adatvédelmi incidens történt, egyébként a 4. blokk végéig törölhető

3. KÁRKOCKÁZATOK FELMÉRÉSE, KÁRENYHÍTÉS

Egyedi vagy tömeges érintettség vélelmezhető?

Egyedi érintettség esetén érintettek

Tömeges érintettség esetén érintetti kategória

Az incidens bekövetkezését elősegítő tényezők

Visszaállíthatóak a megsemmisült, megváltoztatott adatok mentésből?
Van reális esély az elveszetett adatok megtalálására?

Van lehetőség az adatok törlésére, az illetéktelenül tudomást szerzővel titoktartási megállapodás megkötésére további illetéktelen közlések megelőzése céljából?

Van lehetőség a hozzáférés megszüntetésére?

Illetéktelen hozzáférés esetén értelmezhetőek voltak az adatok a hozzáférőnek?

Van olyan logikai intézkedés (pl.jelszócsere) amivel megelőzhetőek a további károk?

Van olyan fizikai intézkedés (pl. zárcsere) amivel megelőzhetőek a további károk?

Van olyan adminisztratív intézkedés (pl. közlemény közzététele, törlési nyilatkozat bekérése, titoktartási megállapodás megkötése) amivel megelőzhetőek a további károk?

Milyen lehetséges hátrányok érhetik az érintetteket az incidens hatására?

Az incidens kapcsán végrehajtott intézkedések

4. TOVÁBBI SZÜKSÉGES KÁRENYHÍTÉS - CSELEKVÉSI TERV

Továbbra is fennáll bármilyen kockázat az érintettekre nézve?

ha igen, az adatvédelmi incidens jelentése szükséges a Hatóságnak

A fennálló kockázat magas kockázatnak minősíthető az érintettre nézve?

ha igen, az érintettel meg kell próbálni felvenni a kapcsolatot, vagy közleményc formájában szükséges tájékoztatni az érintett kört a lehetséges kockázatról

Egyéb megállapítások, szükséges intézkedések

További szükséges intézkedések (pl. feljelentés megtétele)

Mellékletek

Kelt: Budapest, [kitöltendő]

Esemény kivizsgálásában részt vevő személyek:

Név:	Pozíció:
Név:	Pozíció:
Név:	Pozíció:
Név:	Pozíció:

9. melléklet

Adatvédelmi incidens nyilvántartás

Sorszám	Az adatvédelmi incidens rövid megnevezése	Az adatvédelmi incidensről való tudomásszerzés időpontja	Az adatvédelmi incidens bekövetkezésének napja (mikor történt)	A bejelentő megnevezése (adatfeldolgozó, munkavállaló, stb.)	Az incidens körülményeinek, a tények leírása	Kik az érintettek, akiknek az adatait incidens érte	Milyen személyes adatok érintettek az incidenssel	Érintett információs rendszer	Az incidens okának leírása	Az incidens hatásai (valószínű kockázatok, következmények)	Az orvoslásra tett intézkedések listája/leírása, valamint annak hatása	Az incidensről a hatóság, illetve az érintettek tájékoztatásra kerültek-e, amennyiben nem, úgy ennek indoka és magyarázata