

**A Nemzeti Örökség Intézete főigazgatójának
8/2025. (II. 28.) szabályzata
a Nemzeti Örökség Intézete Adatkezelési Szabályzatáról**

Tartalomjegyzék

I. fejezet	4
Bevezető rendelkezések	4
1. A szabályzat célja.....	4
2. A szabályzat hatálya	4
3. Értelmező rendelkezések.....	4
II. fejezet	6
Általános rendelkezések	6
4. Általános alapelvek és szabályok.....	6
5. Az Adatkezelő vezetőjének jogállása, feladat- és hatásköre, felelőssége az adatvédelem tekintetében	7
6. Az Adatkezelő adatvédelmi tisztviselőjének feladatköre és felelőssége	7
III. fejezet	9
Az Adatkezelő által vezetett nyilvántartások	9
7. Adatkezelési tevékenységek nyilvántartása	9
8. Előzetes tájékoztatás kötelezettsége	10
9. Érintetti joggyakorlás.....	11
10. A feladatok megoszlása az érintetti joggyakorlás során	11
11. Hozzáféréshez való jog	12
12. Másolatkéréshez való jog	12
13. Helyesbítéshez való jog.....	13
14. Törléshez való jog	13
15. Elfeledtetéshez való jog	13
16. Korlátozáshoz való jog	14
17. Adathordozhatósághoz való jog	15
18. A tiltakozás joga.....	15
19. Az érintett azonosítása.....	16
20. A kérelem teljesítésének határideje.....	16
21. Az érintetti kérelem teljesítése.....	16
22. Az érintetti kérelem megtagadása	17
23. Az adatvédelmi incidensek kezelése	17
24. Adatbiztonsági intézkedések.....	21
25. A munkáltatói adatkezelésekre vonatkozó közös szabályok.....	22
26. A foglalkoztatottakra vonatkozó adatkezelések.....	23
27. A hivatali e-mail fiók, számítástechnikai eszköz és internet használatának, illetve az otthoni munkavégzés szabályai, valamint a munkáltatói ellenőrzés keretei	24
28. Az Adatkezelő feladataival vagy tevékenységével kapcsolatba kerülő személyekre vonatkozó adatkezelések	26

29. Adatfeldolgozói tevékenység	26
30. Oktatás, tájékoztatás	27
31. Felülvizsgálat.....	27
32. Panasztételi lehetőség	28
IV. fejezet	28
Záró rendelkezések	28
1. melléklet a 8/2025. (II. 28.) szabályzathoz.....	30
Adatkezelési Nyilvántartásba vetési formanyomtatvány	30
2. melléklet a 8/2025. (II. 28.) szabályzathoz.....	31
Érintett tájékoztatása adatvédelmi incidensről formanyomtatvány	31
3. melléklet a 8/2025. (II. 28.) szabályzathoz.....	32
Jegyzőkönyv adatvédelmi incidensről.....	32

**A Nemzeti Örökség Intézete főigazgatójának
8/2025. (II. 28) szabályzata**

a Nemzeti Örökség Intézete Adatkezelési szabályzatáról

A Nemzeti Örökség Intézete (a továbbiakban: Adatkezelő vagy NÖRI) Adatkezelési Szabályzatát (továbbiakban: Szabályzat) az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény, az Európai Parlament és a Tanács (EU) 2016. április 27-i, a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről szóló 2016/679 rendeletének (a továbbiakban: GDPR rendelet) 37. cikk (1) bekezdése alapján az alábbiak szerint határozom meg:

**I. fejezet
Bevezető rendelkezések**

1. A szabályzat célja

1. A NÖRI annak érdekében, hogy a munkatársaira, a partnereire és más érintettekre vonatkozó jogszabályokból fakadó adatvédelmi kötelezettségeit jogszerűen és tisztességesen, valamint az érintett számára átlátható módon végezze, jelen belső szabályzatot alkotja.

2. A szabályzat hatálya

2. A Szabályzat személyi hatálya kiterjed Adatkezelőnél foglalkoztatott valamennyi közalkalmazottra, munkavállalóra, valamint a munkavégzésre irányuló egyéb jogviszony keretében foglalkoztatottakra, továbbá azon személyekre, akik szakmai gyakorlatukat, közösségi szolgálatukat az Adatkezelőnél töltik ill. teljesítik (a továbbiakban együttesen: foglalkoztatott).

3. A Szabályzat tárgyi hatálya kiterjed az Adatkezelő valamennyi adatkezelésére, amely személyes adatra, közérdekű vagy közérdekből nyilvános adatra vonatkozik, az adatkezelés céljától, az adatkezelés típusától és az adatkezelés során alkalmazott eljárástól függetlenül.

3. Értelmező rendelkezések

4. Jelen Szabályzat alkalmazásában:

- a) Adataiany/érintett: bármely meghatározott személyes adat alapján azonosított vagy egyébként – közvetlenül vagy közvetve – azonosítható természetes személy. A személy különösen akkor tekinthető azonosíthatónak, ha őt – közvetlenül vagy közvetve – név, azonosító jel, illetőleg egy vagy több, fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző tényező alapján azonosítani lehet.
- b) Adatfeldolgozó: a NÖRI nevében személyes adatok kezelését végző foglalkoztatott;
- c) Adathordozó: Olyan fizikai eszköz, közeg, amely alkalmas adatok megőrzésére, tárolására. Az adathordozó lehet papír alapú, optikai, mágneses, elektronikus, magneoptikai elven működő eszköz.

- d) Adatkezelés: a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés, továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés;
- e) Adatkezelés korlátozása: a tárolt személyes adatok megjelölése jövőbeli kezelésük ideiglenes beszüntetése céljából;
- f) Adatkezelő: az a természetes vagy jogi személy, jogi személyiséggel nem rendelkező szervezet, 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; jelen szabályzat szempontjából elsődlegesen a NÖRI;
- g) Adatvédelmi incidens: a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi;
- h) Álnevesítés: a személyes adatok olyan módon történő kezelése, amelynek következtében további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik, feltéve hogy az ilyen további információt külön tárolják, és technikai és szervezési intézkedések megtételével biztosított, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet kapcsolni;
- i) Címzett: az a természetes vagy jogi személy, jogi személyiséggel nem rendelkező szervezet, 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;
- j) Érintett hozzájárulása: az érintett akaratának önkéntes, konkrét, megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel az érintett nyilatkozik vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez;
- k) Harmadik fél: az a természetes vagy jogi személy, jogi személyiséggel nem rendelkező szervezet, amely nem azonos az érintettel, az adatkezelővel, az adatfeldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére felhatalmazást kaptak;
- l) Profilalkotás: személyes adatok automatizált kezelésének bármely olyan formája, amelynek során a személyes adatokat valamely természetes személyhez fűződő bizonyos személyes jellemzők értékelésére, különösen a munkahelyi teljesítményhez, gazdasági helyzetéhez, egészségi állapothoz, személyes preferenciákhoz, érdeklődéshez, megbízhatóságához, viselkedéshez, tartózkodási helyhez vagy mozgáshoz kapcsolódó jellemzők elemzésére vagy előrejelzésére használják;
- m) Személyes adat: azonosított vagy azonosítható természetes személyre („érintett”) vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható;

- n) Szervezeti egység: a NÖRI-n belül működő valamennyi igazgatóság és a Főigazgatói Titkárság.

5. Jelen Szabályzatban nem rögzített fogalmak tekintetében a GDPR 4. cikkében meghatározottak az irányadóak.

II. fejezet **Általános rendelkezések**

4. Általános alapelvek és szabályok

6. Adatkezelést jogszerűen és tisztességesen, az érintett számára átlátható módon (jogszerűség, tisztességes eljárás és átláthatóság elveinek mentén) kell végezni:
- a) személyes adatokat az Adatkezelő csak valamelyik, a GDPR 6. cikke szerinti jogalap mentén kezelheti;
 - b) a jogalapot előzetesen, az adatkezelést megelőzően kell kiválasztani.
7. A személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történhet, a céltól eltérő módon történő adatkezelés tilos (célhoz kötöttség):
- a) az adatkezelést az Adatkezelő csak meghatározott, egyértelmű és jogszerű célból folytathatja;
 - b) a személyes adatokat az Adatkezelő nem kezelheti ezekkel a célokkal össze nem egyeztethető módon;
 - c) az adatkezelés célját előzetesen, az adatkezelést megelőzően kell meghatározni.
8. Csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen és a cél elérésére alkalmas (adattakarékosság):
- a) az adatkezeléseknek a céljai szempontjából megfelelőek és relevánsak kell, hogy legyenek, és a szükségesre kell korlátozódniuk;
 - b) az Adatkezelő meg kell előznie a személyes adatok készletezését;
 - c) az adatkezelést annak céljának elérése, teljesülése vagy ellehetetlenülése esetén meg kell szüntetni, az érintett személyes adatokat meg kell semmisíteni.
9. Az adatoknak pontosnak és szükség esetén naprakésznek kell lenniük (pontosság):
- a) a személyes adatoknak pontosnak és szükség esetén naprakésznek kell lenniük: az Adatkezelő köteles minden észszerű intézkedést megtenni annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul töröljék vagy helyesbítsék;
 - b) az adatkezelést végző munkatárs az adatok rögzítésekor ellenőrzi, hogy a megadott adatok megfelelnek-e azoknak az adatfajtáknak, amelyeket az Adatkezelő az adott cél teljesítése érdekében kezelni szándékozik. Az adatkezelést végző munkatárs megtekintésre elkérheti az érintett személyazonosságát igazoló okiratait a pontatlanság feloldása és orvoslása érdekében;
 - c) pontatlan adatok kezelése esetén az adatkezelést végző munkatárs az adatkezelés céljára, valamint a pontatlan adatok kezelésének egyedi sajátosságaira tekintettel haladéktalanul intézkedik a pontatlanul kezelt adatok javítása, vagy adott esetben törlése felől;
 - d) az adatkezelést végző munkatárs intézkedik az adatok frissítését illetően, amennyiben a kezelt adatokkal összefüggő műveletek megtétele során azt tapasztalja, hogy az érintett által megadott adat bármely tekintetében eltér a korábban megadottól.

10. Az adatkezelés céljainak eléréséhez szükséges ideig szabad csak kezelni az adatokat (korlátozott tárolhatóság): a személyes adatok tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé.

11. Megfelelő technikai és szervezési intézkedésekkel biztosítani kell a személyes adatok biztonságát és védelmét (integritás és bizalmas jelleg): a személyes adatok kezelését oly módon kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve.

12. Az Adatkezelő felelős az alapelveknek való megfelelésért, továbbá képesnek kell lennie ennek bizonyítására (elszámoltathatóság): az Adatkezelő felelős a GDPR-ban foglalt követelményeknek való megfelelésért, az adatkezelésekre irányadó szabályok betartásáért. Az Adatkezelőnek képesnek kell lennie a GDPR-nak, valamint a jelen szabályzatban foglaltaknak való megfelelés igazolására.

13. Az Adatkezelő a működése során a jelen alcímben foglalt alapelveknek való megfelelésre törekszik, annak mindenkorai szem előtt tartásával tervezi meg az adatkezeléseit, mely hozzáállás az Adatkezelő foglalkoztatottjaival szemben is elvárás.

5. Az Adatkezelő vezetőjének jogállása, feladat- és hatásköre, felelőssége az adatvédelem tekintetében

14. A főigazgató feladat- és hatásköre:

- a) az Adatkezelő által folytatott adatkezelések jogszerűségének biztosítása;
- b) a jogszabály által a feladat- és hatáskörébe utalt adatkezelési rendszerek egészének (nyilvántartások, adattárak, munkafolyamatok, információáramlások és feldolgozások, jogosultságok) kialakítása és irányítása, rendeltetésszerű működtetése, időszakos felülvizsgálata;
- c) a személyes adatok megfelelő biztonságának biztosítása érdekében az adatkezelések szervezeti és működési feltételeinek kialakítása, a működési és adatbiztonsági követelmények érvényre juttatásának biztosítása;
- d) a NAIH-tól érkező megkeresések ügyében történő intézkedés;
- e) az érintettek jogai érvényesülésének biztosítása érdekében az érintettek megfelelő tájékoztatására, valamint az érintetti kérelmek határidőben történő elbírálására alkalmas eljárásrend kialakítása, melynek szabályait az érintetti joggyakorlásról szóló fejezet tartalmazza;
- f) az adatvédelmi és adatbiztonsági szabályok gyakorlati érvényesülésének ellenőrzése, adatvédelmi feladatok ellátásának felügyelete, illetve intézkedés a hiányosságok felszámolására;
- g) az adatvédelmi tisztviselő támogatása a feladatai ellátásában azáltal, hogy biztosítja számára azokat a forrásokat, amelyek e feladatok végrehajtásához, a személyes adatokhoz és az adatkezelési műveletekhez való hozzáféréshez szükségesek

6. Az Adatkezelő adatvédelmi tisztviselőjének feladatköre és felelőssége

15. Az adatvédelmi tisztviselő a GDPR-ban meghatározott jogállással és feladatkörrel rendelkezik. Az adatvédelmi tisztviselő segíti az Adatkezelőt a GDPR-nak való megfelelésben, támogatást nyújt többek között az adatkezelési tájékoztatók rendszeres felülvizsgálata,

érdekmérlegelési tesztek elvégzése stb. útján az elszámoltathatóság eszközeinek végrehajtásában, valamint közvetítő szerepet tölt be az érdekelt felek (felügyeleti hatóság, érintettek, az Adatkezelő) között adatvédelmi kérdésekben. Az Adatkezelőnél az adatvédelmi tisztviselői feladatokat – megbízási jogviszony alapján – külső szakértő látja el.

16. Az adatvédelmi tisztviselő ellátja a személyes adatok védelmével és a közérdekű adatok nyilvánosságával kapcsolatos feladatokat, ezek az erről szóló megbízási szerződésben kerültek rögzítésre.

17. Az adatvédelmi tisztviselő feladatai:

- a) tájékoztatást nyújt és szakmai tanácsot ad a vonatkozó Európai Uniós és hazai jogszabályokban foglalt adatvédelmi rendelkezések szerinti kötelezettségekről;
- b) figyelemmel kíséri az adatvédelemmel és információszabadsággal összefüggő jogszabályváltozásokat, ellenőrzi a személyes és közérdekű adatok kezelésére vonatkozó jogszabályok és belső szabályozó eszközök érvényesülését;
- c) közreműködik, valamint segítséget nyújt az adatkezeléssel összefüggő döntések meghozatalában, valamint az érintettek jogainak biztosításában;
- d) közreműködik az adatvédelmi hatásvizsgálat lefolytatásában;
- e) a Jogi és Humánpolitikai Igazgatósággal (a továbbiakban: JHI) együtt gondoskodik a belső adatkezelési szabályzat folyamatos aktualizálásáról;
- f) a JHI-val együttműködve gondoskodik az adatvédelmi nyilvántartás és az adatvédelmi incidensek nyilvántartásának vezetéséről;
- g) adatvédelmi incidens bekövetkezése esetén haladéktalanul intézkedik annak kezelésében, valamint szükség esetén ellátja NAIH részére történő bejelentéssel, valamint az érintett tájékoztatásával kapcsolatos feladatokat;
- h) a feladatkörébe tartozó, munkatársak részéről érkező bejelentéseket kivizsgálja, valamint kivizsgálásra továbbítja az illetékes szervezeti egység vezetőjének, valamint ellenőrzi a bejelentés tárgyában tett intézkedést;
- i) kapcsolatot tart a NAIH-al és az érintettekkel, más szervekkel;
- j) a JHI-val együttműködve nyilvántartást vezet az elutasított közérdekű adatigénylések számáról és az elutasítások indokairól, illetve közreműködik a JHI-val abban, hogy a NÖRI eleget tegyen minden év január 31-ig a NAIH felé történő közérdekű adatigénylésekről szóló jelentés teljesítésében;
- k) az Adatkezelő ezirányú írásbeli felhatalmazása birtokában bejelenti a NAIH részére az adatvédelmi tisztviselő adatait (név, postai és elektronikus levélcím) és azok változását, továbbá intézkedik ezen adatok Adatkezelő honlapján történő közzététele érdekében;
- l) kérés esetén a JHI-val együttműködve állásfoglalást ad az Adatkezelő szervezeti egységei részére az adatok nyilvánossága, megismerhetősége tárgyában;
- m) felügyeli az adatkezelő szerv adattovábbítási tevékenységét, különös tekintettel a nemzetközi együttműködés keretében továbbítandó személyes adatokra, felkérésre adatvédelmi szempontból állást foglal az adatok továbbításának jogszerűségével kapcsolatban;
- n) közreműködik a JHI-val és a kérelem tárgyában érintett szakterülettel az érintett bármely (pl. hozzáférési, törlési, tiltakozáshoz fűző stb.) joga gyakorlására vonatkozó kérelmére;
- o) a beérkezett közérdekű adatigénylésekre – a JHI-val együttműködve – elkészíti a választervezetet az Infotv. által előírt határidőben;
- p) ellátja mindazon feladatokat, amelyeket a hatályos adatvédelmi jogszabályok és a megbízási szerződés részére feladatként meghatároz.

18. Az adatvédelmi tisztviselő az adatkezelési rendelkezések betartásának ellenőrzésére jogosult, így az ellenőrzés érdekében minden olyan helyiségbe beléphet, ahol adatkezelés folyik, az adatkezelést végzőktől minden olyan kérdésben felvilágosítást kérhet, minden olyan adatkezelést megismerhet, vagy abba betekinthez, amely az Adatkezelő adatkezelési tevékenységével összefügg.

19. Az ellenőrzés során feltárt hiányosságokról, esetleges jogszabály- vagy normasértésekről az adatvédelmi tisztviselő az ellenőrzés befejezését követően írásban köteles tájékoztatni az Adatkezelő vezetőjét, aki köteles haladéktalanul megtenni a jogszerű állapot helyreállításához szükséges intézkedéseket, valamint indokolt esetben elrendeli vagy kezdeményezi a személyi felelősség megállapításához szükséges eljárás lefolytatását.

20. Az Adatkezelő adatvédelmi tisztviselőjének elérhetőségét a honlapján közzéteszi.

III. fejezet

Az Adatkezelő által vezetett nyilvántartások

7. Adatkezelési tevékenységek nyilvántartása

21. Az Adatkezelő által kezelt, személyes adatot tartalmazó adatkezelések nyilvántartásba vételét az érintett szervezeti egység az 1. melléklet szerinti adatlap JHI részére történő megküldésével kezdeményezi. Az érintett szervezeti egység köteles gondoskodni az általa kezelt személyes adatok vonatkozásában az adatvédelmi tevékenységek két évente esedékes felülvizsgálatáról, valamint szükség szerinti aktualizálásáról, mely aktualizált adatlapot (1. melléklet) haladéktalanul továbbítani köteles a JHI részére.

22. Adatfeldolgozói tevékenységek nyilvántartása: a NÖRI más adatkezelő nevében (adatfeldolgozóként) végzett adatkezelési tevékenységek minden kategóriájáról vezetett nyilvántartásba vételét az érintett szervezeti egység a JHI bevonásával kezdeményezi.

23. Közérdekű adatigénylések nyilvántartása: Az Info tv. 30. § (3) bekezdése alapján a JHI minden év január 31-éig tájékoztatást ad a NAIH számára az előző évben elutasított adatigénylésekről, az elutasítás indokának megjelölésével. A jelentéstételhez a NAIH által a honlapján közzétett nyomtatványt kell alkalmazni, illetve a NAIH aktuális közleménye szerint kell eljárni.

24. Adatvédelmi incidensek nyilvántartása: az Adatkezelő által kezelt adatokkal összefüggésben felmerült adatvédelmi incidensekről vezetett nyilvántartás az alábbiakat tartalmazza: az incidens:

- a. leírását, bekövetkezésének körülményeit (helye, időpontja, oka stb.);
- b. hatásait (érintetti jogok sérülése, érintetti kör nagysága stb.);
- c. kezelésére tett intézkedéseket (kezelés módja, időpontja, NAIH felé történő bejelentés, érintett értesítése esetén ennek ténye stb.).

25. Az Adatkezelő jelen címben felsorolt nyilvántartásait a JHI vezeti és tárolja.

8. Előzetes tájékoztatás kötelezettsége

26. Az Adatkezelő a tájékoztatási kötelezettségét az érintettek és a foglalkoztatottak tájékoztatása céljából elkészített adatkezelési tájékoztatók megalkotásával és nyilvánosságra hozatalával vagy közlésével teljesíti. Kivételesen elfogadható az eseti tájékoztatás nyújtása is a címzettnek.

27. Az adatkezelési tájékoztatót könnyen hozzáférhető formában kell rendelkezésre bocsátani, így elsődlegesen az Adatkezelő honlapján nyilvánosságra kell hozni vagy a helyben szokásos és általában ismert módon közzé kell tenni. A foglalkoztatottnak címzett adatkezelési tájékoztatót a helyben szokásos és általában ismert módon közzé kell tenni, így adott esetben elérhetővé kell tenni belső hálózaton, vagy ki kell függeszteni a hirdetőtáblára, vagy továbbítani kell a belső levelezőrendszeren keresztül.

28. A szervezeti egységek vezetői kötelesek gondoskodni arról, hogy a feladatellátásukkal kapcsolatos valamennyi adatkezelésről – amennyiben az szükséges – az érintettek kifejezett tájékoztatást kapjanak. Az érintettek tájékoztatásáról a személyes adatok kezelésének konkrét körülményeit tekintetbe véve, a személyes adatok megszerzésétől számított észszerű határidőn, de legkésőbb egy hónapon belül kell gondoskodni.

29. Az adatkezelési tájékoztatónak átláthatónak, közérthetőnek, tömörnek kell lennie: tartalmát bekezdésekre kell tagolni, és ahol szükséges, felsorolást kell alkalmazni a szöveg könnyebb áttekinthetősége, olvashatósága érdekében.

30. Amennyiben az Adatkezelő a személyes adatokat az érintettől veszi fel (ilyennek minősül az érintett által a honlapon megadott adatok vagy a foglalkoztatott szóbeli közlése alapján rögzített adatok), akkor az adatkezelési tájékoztatónak az alábbi adatkezelési körülményekre kell kiterjednie:

- a. az Adatkezelő neve, székhelye, központi e-mail címe, illetve az adatvédelmi tisztviselő neve és elérhetősége,
- b. az adatkezelés célja, jogalapja, illetve a személyes adatok tárolásának időtartama, vagy ha ez nem lehetséges, akkor ezen időtartam meghatározásának szempontjai,
- c. a személyes adatok címzettjei, vagy a címzettek kategóriái, ha van ilyen,
- d. az érintett azon joga, hogy kérelmezheti az Adatkezelőtől a rá vonatkozó személyes adatokhoz való hozzáférést, azok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat a személyes adatok kezelése ellen, valamint az érintett adathordozhatósághoz való joga,
- e. a NAIH-nak címzett panasz benyújtásának joga, a NAIH elérhetőségi adatainak feltüntetésével,
- f. automatizált döntéshozatal ténye, ideértve a profilalkotást is, valamint legalább ezekben az esetekben az alkalmazott logikára és arra vonatkozó érthető információk, hogy az ilyen adatkezelés milyen jelentőséggel, és az érintettre nézve milyen várható következményekkel bír,
- g. a GDPR 6. cikk (1) bek. a) pontja, vagy a 9. cikk (2) bekezdésének a) pontja szerinti jogalap (hozzájárulás) alkalmazása esetén a hozzájárulás bármely időpontban történő visszavonásához való jog, illetve az arra vonatkozó tájékoztatás, hogy ez nem érinti a visszavonás előtt a hozzájárulás alapján végrehajtott adatkezelés jogszerűségét,
- h. a GDPR 6. cikk (1) bek. b) pontja szerinti jogalap (szerződés teljesítése) alkalmazása esetén a szerződés lényegére és alapvető céljára vonatkozó információk, illetve az adatszolgáltatás elmaradásának következményei,

- i. a GDPR 6. cikk (1) bek. c) pontja szerinti jogalap alkalmazása esetén a jogi kötelezettség bemutatása, illetve annak forrása (jogszabály neve, jogszabályi szakasz megjelölése, konkrét jogszabályi rendelkezések),
- j. a GDPR 6. cikk (1) bek. f) pontja szerinti jogalap (jogos érdek) alkalmazása esetén az adatkezelő vagy harmadik fél jogos érdekei, valamint az érdekmérlegelési teszt eredménye (azaz, hogy miért élveznek az érdekek elsőbbséget az érintettek érdekeivel, alapvető jogaival és szabadságaival szemben).

31. Amennyiben az Adatkezelő a személyes adatokat nem az érintettől veszi fel, hanem más forrásból szerzi meg (ilyenek minősül amennyiben az érintett adatát továbbítják az Adatkezelő számára), akkor az adatkezelési tájékoztatónak ki kell terjednie:

- a. a személyes adatok kategóriáira, illetve
- b. a személyes adatok forrására.

32. A mindenkori adatkezelési tájékoztatókat a jelen szabályzat 140. pontja szerint tárolja a JHI.

9. Érintetti joggyakorlás

33. Főszabály szerint minden érintett természetes személy hozzáférhet a saját, NÖRI által kezelt személyes adataihoz; az érintettől eltérő személy adataira vonatkozó kérelmeket el kell utasítani, illetőleg amennyiben a kérelem teljesítésével más személy adatai is megismerésre kerülnének, az érintettől eltérő személy adatait ki kell takarni. Az érintett a törvényes képviselője alatt álló kiskorúról kezelt személyes adatokhoz is hozzáférést kérhet, de minden hozzáférési kérelem teljesítésekor vizsgálnia kell a kérelem jogosságát; törvényes képviselő hiányában a hozzáférést bizonyos (pl. egészségügyi) adatokra vonatkozóan meg kell tagadnia. Mivel a Ptk. 4:175. § (2) bekezdése szerinti lényeges kérdésekben a különálló szülők közösen gyakorolják jogukat, annak hitelt érdemlő igazolása is szükséges, hogy közös szülői felügyelet esetén a kérelemben foglaltak mindkét szülő szándékaival egybe esnek.

10. A feladatok megoszlása az érintetti joggyakorlás során

34. Az érintett által benyújtott valamely – 11-18. cím alatt körülírt – jogának gyakorlására irányuló kérelem elbírálása és megválaszolása az Adatkezelő kérelemmel érintett adatkezelést végző szervezeti egységének (a továbbiakban: adatgazda) a feladata. A kérelem elbírálásába és megválaszolásába az adatgazdák a JHI-t és az Adatkezelő adatvédelmi tisztviselőjét kötelesek haladéktalanul bevonni.

35. Az a szervezeti egység, amelyhez a kérelem benyújtásra került – függetlenül attól, hogy adatgazda-e –, köteles a kérelmet 3 munkanapon belül a JHI részére megküldeni, amely azt haladéktalanul továbbítja az Adatkezelő adatvédelmi tisztviselőjére.

36. Az adatvédelmi tisztviselő feladata az érintettnek küldendő válaszlevél tervezetének a kialakítása, illetve a kérelemnek megfelelő intézkedések körének meghatározása, melyet illetően javaslattal él a JHI számára. Az adatvédelmi tisztviselő kérésére a foglalkoztatottaknak, illetve az Adatkezelő által megbízott külső partnereknek közre kell működniük a tervezet megfelelő kialakításában. Az adatvédelmi tisztviselő által elkészített tervezetet a JHI véleményezi, illetőleg a JHI vezetője kiadmányozza. A válaszlevél megküldéséről a JHI vezetőjének választása szerint a JHI vagy az adatgazda gondoskodik.

11. Hozzáféréshez való jog

37. Amennyiben az érintett a hozzáféréshez való jogát gyakorolja (vagy tájékoztatást kér a személyes adatait érintő adatkezelésekről), akkor az Adatkezelőnek tájékoztatást kell nyújtania arról, hogy:

- a. pontosan mely személyes adatait is kezeli az érintettnek; ebben az esetben nem elegendő az adatok kategóriájának megnevezése, a konkrét személyes adatot kell megjelölni;
- b. az Adatkezelő mely cél(ok) mentén megvalósuló adatkezelés(eke)t folytat az érintett vonatkozásában, illetve ezeknek az adatkezeléseknek mi a célja és a jogalapja;
- c. az adatkezelés tárolásának mi az időtartama, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjai;
- d. kiknek továbbítja a személyes adatokat az adatkezelő;
- e. az érintettet az adatkezeléssel összefüggésben megillető jogokról: kérelmezheti az adatkezelőtől a rá vonatkozó személyes adatok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen;
- f. amennyiben nem az érintettől vették fel a személyes adatokat, akkor azok forrásáról;
- g. ha az adatokat nem az érintettől gyűjtötték, a forrásukra vonatkozó minden elérhető információ;
- h. automatizált döntéshozatal tényéről, ideértve a profilalkotást is, valamint legalább ezekben az esetekben az alkalmazott logikára és arra vonatkozó érthető információk, hogy az ilyen adatkezelés milyen jelentőséggel, és az érintettre nézve milyen várható következményekkel jár,
- i. a NAIH-nak címzett panasz benyújtásának jogáról.

38. Ha az érintett a hozzáféréshez való jog teljesítésében más eljárást ajánl fel, és azt az Adatkezelő vállalja, akkor a kérelem az érintett által megjelölt módon is teljesíthető. Az Adatkezelő is az érintett kérelme teljesítésének más módját ajánlhatja fel az érintettnek. Ilyennek tekinthető különösen az érintett személyes adataiba történő betekintés lehetőségének biztosítása.

12. Másolatkéréshez való jog

39. Amennyiben az érintett kérése kifejezetten arra irányul, hogy másolatot kér a személyes adatairól, akkor az Adatkezelőnek az érintett rendelkezésére kell bocsátania a személyes adatok másolatát.

40. A másolat kéréséhez való jogot a következők szerint kell teljesíteni:

- a. papír alapon tárolt személyes adatok esetében a dokumentum fénymásolata vagy szkennelése útján,
- b. elektronikus úton tárolt személyes adatok esetében elektronikus adathordozóra való kimentéssel vagy kinyomtatással.

41. Ha az érintett a másolat kéréshez való jog teljesítésében más módszert ajánl fel, és azt az Adatkezelő vállalja, akkor a kérelem így is teljesíthető. Az Adatkezelő az érintett kérelme teljesítésének más módját ajánlhatja fel az érintettnek.

13. Helyesbítéshez való jog

42. Az érintett kérheti, hogy az Adatkezelő a rá vonatkozó pontatlan személyes adatokat helyesbítse.

43. Az érintett kérelme akkor teljesíthető, ha abban megjelölte, hogy mely személyes adat módosítását kéri és a 118. pontban írtak szerint igazolta, hogy mi a helyes személyes adata.

14. Törléshez való jog

44. Az Adatkezelőnek a személyes adatokat az érintett kérésére indokolatlan késedelem nélkül törölnie kell, amennyiben:

- a. a személyes adatokra már nincs szükség abból a célból, amelyből azokat gyűjtötték vagy más módon kezelték;
- b. az érintett a hozzájárulását visszavonta, és az adatkezelésnek nincs más jogalapja,
- c. az érintett tiltakozik az adatkezelés ellen, és nincs elsőbbséget élvező jogszerű ok az adatkezelésre,
- d. az érintett a marketing célú adatkezelés ellen tiltakozik,
- e. a személyes adatok jogellenes kezelését a NAIH vagy bíróság megállapította,
- f. a személyes adatokat az Adatkezelőre alkalmazandó uniós vagy tagállami jogban előírt jogi kötelezettség teljesítéséhez törölni kell.
- g. a személyes adatok gyűjtésére az információs társadalommal összefüggő szolgáltatások kínálásával kapcsolatosan került sor.

45. Az érintett törlési kérelmét az Adatkezelő akkor tagadhatja meg, ha az Adatkezelő bizonyítani tudja, hogy az adatkezelés szükséges:

- a. a véleménynyilvánítás szabadságához és a tájékozódáshoz való jog gyakorlása céljából,
- b. a személyes adatok kezelését előíró, az adatkezelőre alkalmazandó uniós vagy tagállami jog szerinti kötelezettség teljesítése céljából,
- c. közérdekből vagy az Adatkezelőre ruházott közhatalmi jogosítvány gyakorlása keretében végzett feladat végrehajtása céljából szükségesek,
- d. a népegészségügy területét érintő közérdek alapján,
- e. a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból van szükség a személyes adataira; vagy
- f. jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez.

15. Elfeledtetéshez való jog

46. Amennyiben az Adatkezelő a személyes adatokat nyilvánosságra hozta, és a jelen Szabályzat 14. címe értelmében a személyes adatokat törölni kell, akkor az elérhető technológia és a megvalósítás költségeinek figyelembevételével megteszi az észszerűen elvárható lépéseket – ideértve technikai intézkedéseket – annak érdekében, hogy tájékoztassa az adatokat kezelő adatkezelőket, hogy az érintett kérelmezte tőlük a szóban forgó személyes adatokra mutató linkek vagy e személyes adatok másolatának, illetve másodpéldányának törlését.

47. Az elfeledtetéshez való jog gyakorlásának teljesítéséhez szükséges az, hogy az érintett jelölje meg, mely személyes adatát is hozták nyilvánosságra. Amennyiben az érintett ezt a kérelmében nem tüntette fel, akkor az Adatkezelő felveszi az érintettel a kapcsolatot annak érdekében, hogy az érintett megjelölje, hogy az Adatkezelő mely – kérelemmel érintett – személyes adatát is hozta nyilvánosságra.

48. Amennyiben az Adatkezelő a saját honlapján hozta nyilvánosságra a személyes adatokat, akkor ilyen irányú, megfelelően benyújtott kérelem beérkezése esetén azokat onnan el kell távolítani.

49. Amennyiben az Adatkezelő által kezdeményezett eljárás nyomán más adatkezelő is nyilvánosságra hozta a személyes adatokat, akkor ezen adatkezelőt is értesíteni kell arról, hogy a személyes adatokat törölnie kell.

50. Az Adatkezelőnek az érintett által megjelölt személyes adatra rá kell keresnie a Google keresőszolgáltatón keresztül, hogy a Google az Adatkezelő adatkezelésével összefüggésben listázza-e az adott személyes adatot. Amennyiben igen, akkor a Google keresőmotor bejelentő felületén keresztül ("Tartalom eltávolítása a Google-ból") az érintett által megjelölt személyes adat eltávolítását kell kérni.

51. A 45. pontban szereplő kivételeket az elfeledtetéshez való jog gyakorlása esetén szintén alkalmazni kell.

16. Korlátozáshoz való jog

52. Ha az érintett vitatja a személyes adatok pontosságát, az Adatkezelő arra az időtartamra korlátozza az adatkezelést, amíg ellenőrzi a személyes adatok pontosságát. Ebben az esetben az Adatkezelőnek:

- a. az elektronikus úton tárolt, vitatott pontosságú adat esetében korlátozza az adathoz való hozzáférést,
- b. a papír alapon tárolt, vitatott pontosságú adat esetében a többi irattól elkülönítetten, zárt borítékban tárolja a vitatott pontosságú adatot tartalmazó iratot.

53. Ha az érintett kérelme megalapozott, akkor az Adatkezelő a személyes adatot helyesbíti.

54. Ha az adatkezelés jogellenes, és az érintett ellenzi az adatok törlését, akkor kérheti a személyes adatok felhasználásának korlátozását. Ebben az esetben az Adatkezelő:

- a. az elektronikus úton tárolt, vitatott pontosságú adat esetében a személyes adatot külső adathordozóra (így például pendrive vagy cd-lemez) kimentti, és törli az elektronikus úton tárolt adatot az informatikai rendszerből,
- b. a papír alapon tárolt, vitatott pontosságú adat esetében a többi irattól elkülönítetten, zárt borítékban tárolja a vitatott pontosságú adatot tartalmazó iratot, majd azt az érintett által megjelölt időpontban átadja az érintettnek úgy, hogy az Adatkezelőnél nem marad másolat vagy másodpéldány.

55. Az érintett jogosult arra, hogy a kérje az adatkezelés korlátozását, ha az Adatkezelőnek már nincs szüksége a személyes adatokra, de az érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez. Ebben az esetben az Adatkezelő:

- a. az elektronikus úton tárolt, vitatott pontosságú adat esetében a személyes adatot külső adathordozóra (például pendrive vagy cd-lemez) kimentti, és törli az elektronikus úton tárolt adatot az informatikai rendszerből,
- b. a papír alapon tárolt, vitatott pontosságú adat esetében a többi irattól elkülönítetten, zárt borítékban tárolja a vitatott pontosságú adatot tartalmazó iratot, majd azt az érintett által megjelölt időpontban átadja az érintettnek úgy, hogy az Adatkezelőnél nem marad másolat vagy másodpéldány.

56. Az érintettnek a kérelemben meg kell jelölnie, hogy meddig kéri a felhasználás korlátozását. Amennyiben az érintett nem jelölte meg, akkor elektronikus levelezés útján – ha nem áll rendelkezésre e-mail cím, akkor postai úton – fel kell hívni arra, hogy jelölje meg, milyen időtartamra kéri a felhasználás korlátozását.

57. Az érintett jogosult arra, hogy a kérje az adatkezelés korlátozását, amennyiben a tiltakozás jogát gyakorolja. Ebben az esetben az Adatkezelő arra az időtartamra korlátozza az adatkezelést, amíg a tiltakozási kérelmének jogszerűségét megvizsgálja. Az Adatkezelő:

- a. az elektronikus úton tárolt, vitatott pontosságú adat esetében korlátozza az adathoz való hozzáférést,
- b. a papír alapon tárolt, vitatott pontosságú adat esetében a többi irattól elkülönítetten, zárt borítékban tárolja a vitatott pontosságú adatot tartalmazó iratot.

17. Adathordozhatósághoz való jog

58. Ha az adatkezelés jogalapja az érintett hozzájárulása vagy a szerződéses jogalap, és az adatkezelés automatizált módon történik, akkor az érintett jogosult arra, hogy

- a. a rá vonatkozó, általa egy adatkezelő rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja, vagy
- b. ezeket az adatokat egy másik adatkezelőnek továbbítsa anélkül, hogy ezt az Adatkezelő akadályozná.

59. Amennyiben az Adatkezelő és az érintett által megjelölt másik adatkezelő között technikailag megvalósítható, akkor az érintett jogosult arra, hogy kérje a személyes adatok adatkezelők közötti közvetlen továbbítását.

60. Az Adatkezelőnek az 58. pont a. alpont szerinti esetben a személyes adatokat:

- a. az érintett erre irányuló, kifejezett kérése esetén az általa megjelölt elektronikus elérhetőségre továbbítja, vagy
- b. külső adathordozóra (például pendrive vagy cd-lemez) kimentí (a külső adathordozót az érintett is biztosíthatja).

18. A tiltakozás joga

61. Az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból bármikor tiltakozzon személyes adatainak személyes adatainak a GDPR 6. cikk (1) bekezdésének e) pontján (közérdekű adatkezelés) vagy f) pontján (jogos érdek) alapuló kezelése ellen, ideértve a profilalkotást is. Ebben az esetben az adatkezelő a személyes adatokat nem kezelheti tovább, kivéve a 45. pontban írt eseteket.

62. Tiltakozás esetén meg kell vizsgálni az adatkezelés jogalapját, és ha az alapján fennállnak a tiltakozáshoz való jog érvényesíthetőségének feltételei, meg kell vizsgálni azt, hogy az érintett által megjelölt adatkezelés esetében az érintett által hivatkozott tények, érvek miatt az Adatkezelőnek van-e lehetősége arra, hogy a személyes adatokat törölje, vagy az adatkezelést az érintett vonatkozásában megszüntesse.

63. Az Adatkezelő akkor kezelheti tovább a személyes adatokat, ha bizonyítja, hogy

- a. az adatkezelést olyan kényszerítő erejű jogos okok indokolják, amelyek elsőbbséget élveznek az érintett érdekeivel, jogaival és szabadságaival szemben, vagy
- b. az adatkezelés jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódik.

19. Az érintett azonosítása

64. Ha az Adatkezelőnek (adatgazdának) megalapozott kétségei vannak a kérelmet benyújtó természetes személy kilétével kapcsolatban, kérheti az érintett személyazonosságának megerősítését. Ennek során az Adatkezelő az alábbi lépéseket alkalmazhatja:

- a. telefonhívás útján az Adatkezelő számára rendelkezésre álló további személyes adatokra történő rákérdezés, és helyes válaszok esetén a személyazonosság megerősítését el lehet fogadni,
- b. az Adatkezelő arra kéri az érintett, hogy teljes bizonyító erejű magánokiratban (pl. Azonosításra Visszavezetett Dokumentumhitelesítés, azaz AVDH nevű szolgáltatással hitelesített módon) nyújtsa be a kérelmét,
- c. az érintett az Adatkezelő székhelyén bemutatja valamely személyazonosító igazolványát (személyi igazolvány, jogosítvány, útlevél).

65. Amennyiben az érintett a kilétének megerősítésére más módszert ajánl fel, és azt az Adatkezelő vállalja, akkor az is elfogadható a személyazonosság megerősítéseként. Az Adatkezelő maga is felajánlhat más módszert. Az Adatkezelő nem ajánlhatja fel azt, hogy az érintett a személyazonosító okmányának fénymásolatát vagy szkennelt másolatát küldje el az Adatkezelő számára.

20. A kérelem teljesítésének határideje

66. Az Adatkezelő az érintett kérelmét annak beérkezésétől számított 1 hónapon belül teljesíti. A kérelem beérkezésének napja a határidőbe nem számít bele.

67. Szükség esetén, figyelembe véve a kérelem bonyolultságát és a kérelmek számát, ez a határidő további 2 hónappal meghosszabbítható. A határidő meghosszabbításáról az adatkezelő a késedelem okainak megjelölésével a kérelem kézhezvételétől számított 1 hónapon belül tájékoztatja az érintettet.

21. Az érintetti kérelem teljesítése

68. Az Adatkezelő nem teljesíti az érintett kérelmét, ha azt az érintett telefonhívás útján, szóban közli. Az érintettnek csak elektronikus úton vagy papír alapon küldött kérelme teljesíthető, az elszámoltathatóság elvének érvényesülése érdekében. Erről az érintettet az esetleges telefonhívása során tájékoztatni kell.

69. Az Adatkezelőnek olyan módon kell teljesíteni az érintett kérelmét (ideértve a kérelem teljesítéséről vagy elutasításáról szóló tájékoztatást is), amilyen csatornán, illetve formátumban az érintett kéri. Ha az érintett nem jelöli meg egyértelműen a csatornát, illetve formátumot, az Adatkezelő azt a módot választja, amilyen módon az érintett benyújtotta a kérelmét.

70. Ha az érintett elektronikus úton nyújtotta be a kérelmet, és a másolatot is elektronikus formátumban kéri, akkor az Adatkezelőnek a másolatot elektronikus formátumban kell rendelkezésre bocsátani.

71. Az Adatkezelőnek az érintett kérelmében megjelölt érintetti jogot kell teljesíteni. Amennyiben az érintetti kérelem nem pontos, és a kérelem alapján nem lehet eldönteni, hogy milyen jogot kíván az érintett gyakorolni, akkor ennek tisztázása érdekében fel kell venni vele a kapcsolatot.

72. Ha az érintett a kérelmében több jogot is gyakorolni kíván, akkor azok mindegyikét teljesíteni kell (például hozzáféréshez való jog és törléshez való jog egyidejű gyakorlása esetén egyrészt tájékoztatni kell az érintettet arról, hogy milyen személyes adatait kezeli az Adatkezelő, másrészt pedig végre kell hajtani a személyes adatok törlését – amennyiben fennállnak a feltételei –, és erről az érintettet tájékoztatni kell).

73. Az érintett kérelmének teljesítését díjmentesen kell biztosítani.

22. Az érintetti kérelem megtagadása

74. Az érintetti kérelem kizárólag akkor tagadható meg, ha uniós vagy tagállami jogszabály a GDPR 23. cikk (1) bekezdésében felsorolt érdekek védelme miatt korlátozza vagy kizárja az érintetti joggyakorlás teljesítését.

75. Ha az érintett kérelme egyértelműen megalapozatlan vagy – különösen ismétlődő jellege miatt – túlzó, az Adatkezelő megtagadhatja a kérelem alapján történő intézkedést.

76. Az érintett kérelmének megtagadásáért nem lehet díjat felszámítani.

77. Ha az Adatkezelő nem teljesíti az érintett kérelmét, akkor 1 hónapon belül tájékoztatja az érintettet

- a) az intézkedés elmaradásának ténybeli és jogi okairól (mely jogszabály vagy a GDPR mely rendelkezése az, amely alapján jogszerűen tagadja meg a kérelem teljesítést), valamint arról, hogy
- b) az érintett panaszt nyújthat be a NAIH-nál, és élhet bírósági jogorvoslat jogával.

23. Az adatvédelmi incidensek kezelése

78. Adatvédelmi incidensnek minősülnek többek között különösen az alábbiak:

- a. harmadik fél által a személyes adatokat tároló informatikai rendszer vagy adatkezelő szoftverhez történő jogosulatlan hozzáférés – az adat sérült tulajdonsága: bizalmasság,
- b. a személyes adatok jogosulatlan titkosítása, amelynek következtében a személyes adatokhoz – akár átmenetileg – nem lehet hozzáférni vagy az Adatkezelő adatkezelései során felhasználni – az adat sérült tulajdonsága: rendelkezésre állás,
- c. ha az Adatkezelő foglalkoztatottja jogosulatlanul hozzáfér személyes adatokhoz, vagy a jogosultsági szintjét meghaladóan fér hozzá a személyes adatokhoz – az adat sérült tulajdonsága: bizalmasság,
- d. személyes adatok véletlen vagy szándékos, felhatalmazás nélküli nyilvánosságra hozatala – az adat sérült tulajdonsága: bizalmasság,
- e. személyes adatokat tartalmazó dokumentum más számára történő hozzáférhetővé tétele – az adat sérült tulajdonsága: bizalmasság,
- f. személyes adatokat tartalmazó postai küldemény téves címzetthez történő elpostázása – az adat sérült tulajdonsága: bizalmasság,
- g. személyes adatokat tartalmazó e-mail téves címzettnek történő kiküldése – az adat sérült tulajdonsága: bizalmasság,
- h. személyes adatokat tartalmazó adathordozó vagy informatikai eszköz elvesztése – az adat sérült tulajdonsága: bizalmasság,
- i. a személyes adatokat tároló informatikai eszköz vagy az ilyen adatokat tartalmazó dokumentumok sérülése, megsemmisülése (ideértve a tüzesetet vagy a vízkár által

okozott sérülést vagy megsemmisülést), amelynek következtében a személyes adatokhoz - akár átmenetileg - nem lehet hozzáférni vagy az Adatkezelő adatkezelései során felhasználni – az adat sérült tulajdonsága: sértetlenség, rendelkezésre állás.

79. Az adatvédelmi incidenseknek alapvetően három kategóriája különböztethető meg:
- a. bizalmassági incidens;
 - b. sértetlenséggel kapcsolatos incidens és
 - c. rendelkezésre állással kapcsolatos incidens.
80. Az Adatkezelő az adatkezelés megkezdését megelőzően felméri az érintett személyek jogaira és szabadságaira vonatkozó előzetes kockázatot a bizalmasság, sértetlenség, rendelkezésre állás szempontjából, figyelembe véve a kockázat valószínűségét és súlyosságát.
81. Adatvédelmi incidens bekövetkezése esetében a következő lépéseket kell az Adatkezelőnek (szervezeti egységeinek vezetői útján) megtennie:
- a. az adatvédelmi incidens kockázati besorolásának elvégzése az adatvédelmi tisztviselővel együttműködve (legalább azon a szinten, hogy az incidens kockázati szintje: magas vagy nem magas);
 - b. annak eldöntése, hogy az adott incidens milyen kockázatot jelent az érintettek jogaira és szabadságaira vonatkozóan. Az Adatkezelő a kockázatelemzést az incidensről való tudomásszerzést követően megkezdi és egészen az incidens kezelés lezárásig folyamatosan figyelemmel kíséri.
82. Az adatvédelmi incidens kockázatának megítélése során az alábbi szempontokat veszi figyelembe az Adatkezelő:
- a. az incidens jellege;
 - b. az incidenssel érintett személyes adatok jellege, típusa, érzékenysége;
 - c. az incidenssel érintett személyes adatok mennyisége;
 - d. az érintettek azonosíthatósága és száma, sajátosságaik;
 - e. az érintettekre vonatkozó következmények súlyossága;
83. Az Adatkezelőnél adatvédelmi incidens bekövetkezésének észlelése esetén az incidenssel vagy az azzal összefüggő adat kezelésével érintett szervezeti egység vezetője haladéktalanul jelentést tesz a JHI vezetőjének, aki soron kívül értesíti az adatvédelmi tisztviselőt.
84. Adatvédelmi incidensre vonatkozó értesítést követően haladéktalanul fel kell függeszteni azt a gyakorlatot, ami az adatvédelmi incidens hatását fokozná.
85. A felfüggesztés megszüntethető különösen, ha
- a. a rendelkezésre álló információk alapján az adatvédelmi incidensnek nincsenek és nem is várhatóak súlyos következményei, vagy
 - b. a felfüggesztést követően az Adatkezelő olyan intézkedéseket hozott, amelyek biztosítják, hogy az adatvédelmi incidensnek nincsenek és nem is várhatóak súlyos következményei.

86. A felfüggesztés megszüntetéséről az adatvédelmi tisztviselő javaslatára a JHI vezetője és az érintett szervezeti egység vezetője együttesen, vita esetén a főigazgató dönt. A javaslatban ki kell térni arra, hogy

- a. milyen adatvédelmi incidens történt (a személyes adatok típusa, mennyisége, érintettek száma, kategóriái, milyen következményei voltak vagy lehettek volna az érintettre),
- b. miért javasolt a felfüggesztés megszüntetése.

87. Az adatvédelmi tisztviselő haladéktalanul tájékozódik a bekövetkezett adatvédelmi incidens körülményeiről, felméri, hogy az incidens valószínűsíthetően kockázatot eredményez-e az érintettek jogai érvényesülése vonatkozásában, és megteszi a szükséges lépéseket a mielőbbi károk elhárítása érdekében.

88. Amennyiben az adatvédelmi tisztviselő által jóváhagyott kockázatbecslés eredménye alapján az adatvédelmi incidens kockázattal jár az érintettek jogai érvényesülése vonatkozásában, az adatvédelmi tisztviselő lehetőség szerint a tudomásszerzést követő 72 órán belül a NAIH honlapján elérhető adatvédelmi incidensbejelentő rendszeren keresztül (<https://www.naih.hu/index.php/adatvedelmi-incidensbejelento-rendszer>) megteszi a bejelentést, ezzel egyidejűleg jelentést tesz a főigazgató és a JHI vezetője felé a megtett intézkedésekről. Amennyiben a bejelentés nem teljesíthető az előírt határidőben, a NAIH felé történő bejelentésben meg kell jelölni és igazolni kell a késedelemre vonatkozó okokat is.

89. Amennyiben az előzetes vizsgálat alapján egyértelműen megállapítható, hogy az adott esemény nem érintett személyes adatokat, akkor az eseményt nem kell adatvédelmi incidensként kezelni. Ebben az esetben is az előzetes vizsgálat keretében fel kell térképezni, hogy

- a. mi volt az adott esemény oka,
- b. miért nem következett be adatvédelmi incidens, illetve
- c. amennyiben az adott esemény kapcsán értelmezhető – hogyan lehet megelőzni azt, hogy a jövőben ne következzen be hasonló esemény.

90. Abban az esetben, ha bizonyítottan adatvédelmi incidens történt, azonban arról történő tudomásszerzés időpontjában vagy az előzetes vizsgálat alapján megállapítható, hogy az incidensnek valószínűsíthetően nincs meghatározó kockázata az érintetteknek nézve, akkor az incidensről nem kell bejelentést tenni a NAIH-nak. Ilyen adatvédelmi incidensnek tekinthető különösen az, ha a személyes adatokat tartalmazó, az érintett téves lakcímére küldött postai küldemény felbontás nélkül visszaérkezik az Adatkezelőre. Az adatvédelmi incidens bejelentésének mellőzéséről az adatvédelmi tisztviselő és a JHI javaslata alapján a főigazgató dönt. A javaslatban ki kell térni arra, hogy

- a. milyen adatvédelmi incidens történt (a személyes adatok típusa, mennyisége, érintettek száma, kategóriái, milyen következményei voltak vagy lehettek volna az érintettre),
- b. miért nem következett be az érintetteknek nézve kockázatot jelentő adatvédelmi incidens,
- c. amennyiben az adott adatvédelmi incidens kapcsán értelmezhető – hogyan lehet megelőzni azt, hogy a jövőben ne következzen be hasonló adatvédelmi incidens,
- d. miért javasolja azt, hogy erről az Adatkezelő ne tegyen bejelentést a NAIH-nak.

91. Amennyiben a főigazgató a javaslatot elfogadja, nem kell bejelentést tenni, az adatvédelmi incidenst csak fel kell vezetni az adatvédelmi tisztviselő által vezetett incidensnyilvántartásba.

92. Az adatvédelmi incidensről való tudomásszerzésnek az tekinthető, ha a kockázatelemzés alapján a NÖRI, mint adatkezelő észszerű mértékű bizonyosságot szerez arról, hogy olyan esemény történt, amely a személyes adatokkal kapcsolatos jogellenes műveletekhez vezet. Tudomásszerzésnek minősülnek különösen az alábbiak:

- a. az adatvédelmi incidens bekövetkezésére utaló körülményt az Adatkezelő munkatársa fedezi fel,
- b. az Adatkezelőnek e-mailen, postai levélben vagy más kommunikációs eszköz útján küldött üzenet, levél, amely adatvédelmi incidens bekövetkezésére utaló körülményt tartalmaz (abban az esetben is, ha az üzenet vagy a levél névtelen),
- c. az Adatkezelőt telefonon keresztül adatvédelmi incidens bekövetkezésére utaló körülményről értesítik (abban az esetben is, ha a hívó fél ismeretlen vagy névtelen),
- d. a sajtóban vagy más honlapon megjelent, adatvédelmi incidens bekövetkezésére utaló körülmény, amelyről az Adatkezelőt értesül vagy arról értesítik,
- e. az Adatkezelő által megbízott adatfeldolgozó e-mailben vagy telefonon jelzi, hogy az Adatkezelő által kezelt személyes adatokkal összefüggésben adatvédelmi incidens következett be.

93. Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az Adatkezelő késedelem nélkül tájékoztatja az érintettet az adatvédelmi incidensről a 2. melléklet szerinti formanyomtatvány alkalmazásával.

94. Az érintett részére adott tájékoztatásban világosan és közérthetően ismertetni kell az adatvédelmi incidens jellegét, és közölni kell az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit; ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket; ismertetni kell az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

95. Az érintettet nem kell tájékoztatni, ha az Adatkezelő:

- a. megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre, és emiatt a hozzáférésre fel nem jogosított személyek számára értelmezhetetlenek a megszerzett adatok;
- b. az adatvédelmi intézkedést követően olyan további intézkedéseket tett, amelyek biztosítják, hogy az érintett jogaira és szabadságaira jelentett magas kockázat a továbbiakban valószínűsíthetően nem valósul meg;
- c. a tájékoztatás aránytalan erőfeszítést tenne szükségessé.

96. Az adatvédelmi incidens kezelésére az Adatkezelőn belül, ad hoc jelleggel incidenskezelő csoport működik, amelynek tagjai az incidenssel érintett szervezeti egység, a Gazdasági Igazgatóság és a JHI egy-egy munkatársa, valamint az adatvédelmi tisztviselő. Az incidenskezelő csoportban az adatvédelmi tisztviselő a koordinációért és a kapcsolattartásért felelős személy. Az incidenskezelő csoport tagjait a főigazgató jelöli ki.

97. Amennyiben az adatvédelmi incidens sajátosságainál fogva indokolt, az adatvédelmi incidens hatékony kezelése érdekében a főigazgató külső szakértők bevonásáról dönthet.

98. Az adatvédelmi incidenssel érintett szervezeti egység vezetője a 3. melléklet szerinti tartalommal jegyzőkönyvet készít, melyet a JHI részére köteles továbbítani az adatvédelmi incidens nyilvántartásba vétele céljából.

24. Adatbiztonsági intézkedések

99. Az Adatkezelő és az adatfeldolgozó a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja, ideértve, többek között, adott esetben:

- a. a személyes adatok álnevesítését és titkosítását;
- b. a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítását, integritását, rendelkezésre állását és ellenálló képességét;
- c. fizikai vagy műszaki incidens esetén az arra való képességet, hogy a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását kellő időben vissza lehet állítani;
- d. az adatkezelés biztonságának garantálására hozott technikai és szervezési intézkedések hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárást.

100. Az Adatkezelőnél bármely foglalkoztatási jogviszonyban lévő személyek kötelesek jelen Szabályzat, továbbá a hatályos jogszabályok szerint a rájuk bízott, valamint tudomásukra jutott személyes adatokat időbeli korlátozás nélkül megőrizni. A foglalkoztatottak kizárólag a munkaköri leírásban meghatározott feladatkörükön belül ismerhetik meg az ilyen adatokat. E titoktartás nem terjed ki a közérdekű adatok nyilvánosságára és a közérdekből nyilvános adatra vonatkozó, külön törvényben meghatározott adatszolgáltatási és tájékoztatási kötelezettségre.

101. Minden személyes adatot, üzleti titkot tartalmazó rendszerhez való hozzáférésre feljogosított foglalkoztatott köteles titoktartási kötelezettségvállalást tenni. A kötelezettségvállalásban az érintettet nyilatkoztatni kell arról, hogy az Adatkezelő jelen Szabályzatának rendelkezéseit megismerte, a szükséges titokvédelmi ismereteket elsajátította, valamint a személyes adatok védelméhez fűződő jog és az üzleti titok megsértésének mind büntetőjogi, mind polgári jogi következményeivel tisztában van.

102. Az Adatkezelő foglalkoztatottja a munkavégzése során birtokában lévő, a GDPR, az Infotv. és jelen Szabályzat előírásai alapján személyes adatnak minősülő adatokat tartalmazó iratokat köteles munkaidőn túl – és amelyeket lehetséges munkaidőben is – szekrényébe zárva és/vagy zárható szobában eltárolva tartani. Az asztalon és az irodában egyéb helyen hivatalos iratok csak a munkavégzés céljából és kizárólag annak időtartama alatt tárolhatók.

103. A fenti bekezdésben felsorolt iratok elzárásáért az a foglalkoztatott felelős, akinél azok a munkaidő befejezésekor találhatók. Azokat a helyiségeket, ahol közös használatú nyomtató, fénymásológép, szkennerek, valamint egyéb, irat előállítására, fűzésére, laminálására stb. alkalmas berendezés (együttesen a továbbiakban: irodatechnikai eszközök) üzemel, az adatbiztonsági követelmények figyelembevételével kell használni. Az irodatechnikai eszközök használatának befejeztével az iratot a lehető legrövidebb időn belül el kell távolítani az irodatechnikai eszközökből. Az irodatechnikai eszközben maradt iratért adatvédelmi szempontból az felel, aki az iratot az irodatechnikai eszközzel fizikailag előállította, valamint módosította.

104. Azokat a szobákat, a helyiségeket, ahol számítógép, munkaállomás üzemel, úgy kell használni, hogy az megfeleljen az adatvédelmi, tűzrendészeti és informatikai biztonsági követelményeknek. A foglalkoztatott köteles a számítógépet, és az ahhoz alkalmazott adathordozókat úgy kezelni, tárolni, hogy a védelmet igénylő adatokat illetéktelen személy ne ismerhesse meg. Köteles továbbá a munkaidő végeztével a munkaállomást – ettől eltérő utasítás hiányában – kikapcsolni, az iroda ajtaját bezárni.

105. Személyes adatokat is tartalmazó iratot az Adatkezelő székhelyéről kivinni – munkaköri feladat ellátásának kivételével – csak az érintett szervezeti egység vezetőjének engedélyével lehet. A foglalkoztatott ez esetben is köteles gondoskodni arról, hogy az ne vesszen el, ne rongálódjon vagy semmisüljön meg, továbbá tartalma illetéktelen személy tudomására ne jusson.

106. Iratok és adatok mobiltelefonon, valamint egyéb elektronikus úton – és csak a vonatkozó jogszabályi előírások betartásával – kellő körültekintéssel és kizárólag az Adatkezelő technikai eszközeinek igénybevételével továbbíthatók. A személyes adatokat tartalmazó egyéb iratanyagok megsemmisítéséről a szükséges biztonsági intézkedések mellett kell gondoskodni.

107. Az egyes nyilvántartások, adatkezelések tekintetében a hozzáférési jogosultságot a főigazgatónak, illetve a szervezeti egységek vezetőinek kell meghatározni és azok folyamatos nyilvántartásáról gondoskodnia.

108. Az Adatkezelő szervezeti rendszerén belül a személyes adatok – a feladat elvégzéséhez szükséges mértékben és ideig – továbbíthatók olyan szervezeti egységhez, amely ezen adatokkal kapcsolatban további feladatokat lát el.

109. Az egyes adatkezelésekhez a hozzáférési jogosultságot személyre szólóan kell megállapítani. Amennyiben a jogosultság megállapítására alapot adó körülményben változás történik, haladéktalanul intézkedni kell a jogosultság módosítására vagy visszavonására.

110. A jogosultat tájékoztatni kell a jogosultsággal kapcsolatos jogairól és kötelezettségeiről, a vonatkozó szabályok megszegésének következményeiről. A tájékoztatás tényét és tudomásul vételét írásban dokumentálni kell.

111. Az adatok informatikai módszerrel történő tárolási módját úgy kell megválasztani, hogy azok törlése – az esetleg eltérő törlési határidőre is tekintettel – az adattörlési határidő lejártakor, valamint, ha az egyéb okból szükséges, elvégezhető legyen. A törlésnek visszaállíthatatlannak kell lennie.

112. A papír alapú adathordozókat iratmegsemmisítő segítségével, vagy főigazgatói döntés alapján külső, iratmegsemmisítésre szakosodott szervezet igénybevételével kell a személyes adatoktól megfosztani. Elektronikus adathordozók esetében az elektronikus adathordozók selejtezésére vonatkozó szabályok szerint kell gondoskodni a fizikai megsemmisítésről, valamint szükség szerint előzetesen az adatoknak a biztonságos és visszaállíthatatlan törléséről.

25. A munkáltatói adatkezelésekre vonatkozó közös szabályok

113. A munkáltatói adatkezelések esetében érintettek:

- a. az álláshirdetésre jelentkező személyek, ideértve az álláslehetőség iránt megkeresést küldő személyek és a toborzási adatbázisban szereplő személyek,
- b. a foglalkoztatottak, illetve annak közvetlen hozzátartozói.

114. Az Adatkezelő az érintettek személyes adatait a jogviszony létesítésével, teljesítésével, megszűnésével (megszüntetésével) vagy a jogi igény védelmével, érvényesítésével összefüggő adatkezelési célokból kezelheti.

115. A foglalkoztatott kötelezhető a személyes adatait igazoló okiratainak bemutatására, azonban okiratairól az Adatkezelő másolatot sem papír alapon, sem elektronikusan nem készíthet, tekintettel az eredeti okiratok közhiteles jellegére, valamint az adattakarékosság és célhoz kötöttség elveire.

116. A fentiekől eltérően személyes adatokat igazoló okiratról történő másolatkészítésre kizárólag jogszabály felhatalmazása alapján kerülhet sor.

117. A személyes adatokat igazoló okirat bemutatása során az okiratok Adatkezelő ügyintézője általi megtekintéséről és az adatok helyességéről feljegyzés készíthető, melyet az Adatkezelő ügyintézője és a foglalkoztatott együttesen aláír.

26. A foglalkoztatottakra vonatkozó adatkezelések

118. Az Adatkezelő elsődlegesen az alábbi körben végez adatkezelést:

- a. az álláshirdetésre jelentkezőkkel összefüggő adatkezelés,
- b. az álláslehetőség iránti megkereséssel összefüggős adatkezelés,
- c. a toborzási adatbázissal összefüggő adatkezelés,
- d. a munkaszerződés megkötése érdekében szükséges adatok kezelése,
- e. személyes adatok továbbítása az állami adóhatóság felé,
- f. munkaköri alkalmassági vizsgálattal összefüggő adatkezelés,
- g. a pótszabadságra, szülési szabadságra és a fizetés nélküli szabadságra való jogosultság megítélésével összefüggő adatkezelés,
- h. bérszámfejtéssel, a munkabér kifizetéssel, valamint a foglalkoztatotti nyilatkozatokkal összefüggő adatkezelés,
- i. a foglalkoztatott magáncélú elérhetőségek kezelésével összefüggő adatkezelés,
- j. a NÖRI nevében történő kapcsolattartással összefüggő adatkezelés,
- k. az utazások megszervezésével összefüggő adatkezelés,
- l. a vagyonyilatkozat-tételi kötelezettséggel összefüggő adatkezelés,
- m. a magáncélú használat tilalmának megsértésének ellenőrzésével együtt járó adatkezelés,
- n. a titoktartási kötelezettség megsértésének ellenőrzésével együtt járó adatkezelés,
- o. a munkahelyi balesettel összefüggő adatkezelés,
- p. vészhelyzet esetén értesítendő személyre vonatkozó adatkezelés,
- q. a munkáltatói jogkör gyakorláshoz kapcsolódó adatkezelés,
- r. a NÖRI weboldalán megjelenő személyes adatokkal kapcsolatos adatkezelés.

119. Amennyiben a Szabályzat vagy jogszabály nem állapít meg eltérő adatkezelési időtartamot, akkor az Adatkezelő a munkaszerződést, munkavállalói nyilatkozatokat és más, a munkaviszonyra vonatkozó dokumentumokat (a továbbiakban összefoglalóan: munkaügyi iratok) az alábbi időtartamig őrizheti meg:

- a. a kizárólag munkajogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez szükséges munkaügyi iratokat az Mt. 286. §-ában meghatározott elévülési idő elteltéig, főszabály szerint a munkaviszony megszűnésétől számított három évig,
- b. a kizárólag munkaügyi ellenőrzés érdekében szükséges munkaügyi iratokat a munkaügyi ellenőrzésről szóló 1996. évi LXXV. törvény 5/A. §-a szerinti elévülési

- idő elteltéig, főszabály szerint a munkaviszony megszűnésétől számított három évig, (a megszűnést követő 3. év utolsó napja)
- c. a kizárólag polgári jogi igények védelméhez, érvényesítéséhez szükséges munkaügyi iratokat a Polgári Törvénykönyvről szóló 2013. évi V. törvény (a továbbiakban: Ptk.) 6:21.-6:25. §-a szerinti elévülési idő elteltéig, főszabály szerint öt évig,
 - d. a kizárólag adóhatósági ellenőrzés érdekében szükséges munkaügyi iratokat az adózás rendjéről szóló 2017. évi CL. törvény (Art.) 202-205. §-a szerinti elévülési idő elteltéig, főszabály szerint nyolc évig,
 - e. a társadalombiztosítási nyugellátásról szóló 1997. évi LXXXI. törvény 99/A. § (1) bekezdése alapján az Adatkezelő a foglalkoztatott (volt foglalkoztatott) biztosítási jogviszonyával összefüggő, a szolgálati időről vagy a nyugellátás megállapítása során figyelembevételre kerülő keresetről, jövedelemről adatot tartalmazó munkaügyi iratokat a munkavállalóra, volt munkavállalóra irányadó öregségi nyugdíjkorhatár betöltését követő öt évig,
 - f. azon munkaügyi iratokat, amelyet valamely bírósági eljárásban felhasználnak vagy arra hivatkoznak, a bírósági eljárás jogerős lezárásáig (rendkívüli jogorvoslat esetén annak lezárásáig).

120. Amennyiben a munkaügyi irat több kategóriába is tartozhat, akkor a hosszabb megőrzési időtartamot kell alkalmazni az adott munkaügyi iratra.

121. A közalkalmazottak esetében az Adatkezelő elsődlegesen az alábbi adatkezeléseket végzi:

- a. a pályázatra jelentkezőkkel összefüggő adatkezelés,
- b. a büntetlen előélet igazolásával összefüggő adatkezelés,
- c. a közalkalmazotti alapnyilvántartás vezetésével összefüggő adatkezelés,
- d. munkaköri alkalmassági vizsgálattal összefüggő adatkezelés,
- e. a pótszabadságra, szülési szabadságra és a fizetés nélküli szabadságra való jogosultság megítélésével összefüggő adatkezelés,
- f. a központosított illetmény-számfejtési rendszerbe történő adattovábbítás,
- g. a foglalkoztatott magáncélú elérhetőségek kezelésével összefüggő adatkezelés,
- h. az NÖRI nevében történő kapcsolattartással összefüggő adatkezelés
- i. az utazások megszervezésével összefüggő adatkezelés,
- j. a vagyonyilkozat-tételi kötelezettséggel összefüggő adatkezelés,
- k. a magáncélú használat tilalmának megsértésének ellenőrizhetősége,
- l. titoktartási kötelezettség megsértésének ellenőrizhetősége,
- m. a munkahelyi balesettel összefüggő adatkezelés
- n. vészhelyzet esetén értesítendő személyre vonatkozó adatkezelés,
- o. a munkáltatói jogkör gyakorláshoz kapcsolódó adatkezelés
- p. a NORI weboldalán megjelenő személyes adatokkal kapcsolatos adatkezelés.

27. A hivatali e-mail fiók, számítástechnikai eszköz és internet használatának, illetve az otthoni munkavégzés szabályai, valamint a munkáltatói ellenőrzés keretei

122. Az Adatkezelő nevében történő hivatalos levelezés lebonyolításához, illetve a foglalkoztatottak egymás közötti, az Adatkezelő érdekében történő kapcsolattartáshoz az Adatkezelő valamennyi foglalkoztatottja és vezetője számára a vezeték- és keresztnévét tartalmazó e-mail-címet és ehhez tartozó e-mail fiókot biztosít (a továbbiakban: hivatali e-mail fiók). A hivatali e-mail fiók magáncélra történő használata tilos. Magáncélú használatnak minősül többek között bármilyen, nem a foglalkoztatott munkaköréhez, munkavégzéséhez

kapcsolódó vagy nem az Adatkezelő érdekében történő e-mail küldés, illetve fogadás. Az ilyen tartalmú leveleket a foglalkoztatottnak haladéktalanul törölnie kell.

123. Az Adatkezelő a munkavégzés céljából számítógépet, laptopot, tabletet, mobiltelefont, illetve külső adathordozót (a továbbiakban: hivatali számítástechnikai eszközt) bocsáthat a foglalkoztatottak rendelkezésére. A hivatali számítástechnikai eszközt a foglalkoztatott kizárólag munkaköréhez tartozó feladatok ellátására használhatja, ezek magáncélú használatát az Adatkezelő megtiltja. A magáncélú használat mobiltelefon esetén nem tiltott akkor, ha a munkatárs mobiltelefon-használatát nem kizárólag a munkáltató biztosítja (saját készülék céges SIM kártyával és saját számmal vagy DUAL SIM kártyával, céges készülék céges SIM kártyával és saját számmal vagy DUAL SIM kártyával). Magáncélú használatnak minősül különösen az, ha a hivatali számítástechnikai eszközön olyan adatot tárol (így például fényképet, videófelvételt, szöveges dokumentumot), amely nem kapcsolódik a foglalkoztatott munkaköréhez vagy az adatot nem az Adatkezelő érdekében tárolja az eszközön. A foglalkoztatottnak az esetleges magáncélú adatokat legkésőbb a jogviszony megszűnésekor törölnie kell a használatában lévő hivatali számítástechnikai eszközökről, melyről a humánpolitikai eljárásrendről szóló mindenkorai szabályzat szerinti elszámolólapon nyilatkoznia is kell.

124. Az Adatkezelőnél munkaidőben tilos az internet magáncélú használata. Magáncélú használatnak minősül különösen bármilyen, nem a foglalkoztatott munkaköréhez, munkavégzéséhez kapcsolódó vagy nem az Adatkezelő érdekében történő internethasználat. A foglalkoztatottnak haladéktalanul törölnie kell az internet magáncélú használata során keletkező személyes adatokat (így például az elmentett felhasználó neveket, jelszavakat, böngészési előzményeket).

125. Az Adatkezelő, mint munkáltató – kivételesen és annak feltételei fennállása esetén – elrendelheti az otthoni munkavégzést foglalkoztatottai részére. Az otthoni munkavégzés elrendelése esetében

- a. a foglalkoztatottnak kell biztosítania a részére átadott munkaeszközök (laptop, mobiltelefon, USB) biztonságos szállítását és tárolását,
- b. a foglalkoztatottnak a munkaeszközöket úgy kell tárolnia, hogy ahhoz illetéktelen személy ne férhessen hozzá, az eszközökön – ha az a munkáltató által biztosított eszköz – csak a munkáltató által telepített programokat, alkalmazásokat használhatja;
- c. munkavégzés közben az eszközt a foglalkoztatottnak úgy kell használnia, hogy ahhoz harmadik személy ne férjen hozzá;
- d. az otthoni munkavégzésének helyét (ha ez nem lehetséges, akkor otthonát) zárni köteles, ha otthonról eltávozik; a foglalkoztatott köteles gondoskodni a nála lévő munkaeszközök és a munkáltatói hivatalos iratok elzárásáról;
- e. illetéktelen használat észlelése esetén a foglalkoztatott köteles haladéktalanul felvenni a kapcsolatot az Adatkezelő informatikai szakemberével.

126. Az Adatkezelőnek a Mt. 11/A. § (1) bekezdésében biztosított jogszabályi felhatalmazás alapján lehetősége van – előzetes tájékoztatás mellett – annak ellenőrzésére, hogy

- a. a foglalkoztatottak megtartották-e a magáncélú használat tilalmára vonatkozó kötelezettségüket,
- b. a foglalkoztatottak megtartották-e a titoktartási kötelezettségüket.

127. Az Adatkezelő az ellenőrzéssel együtt járó adatkezelését a jogos érdek jogalapjának [GDPR 6. cikk (1) bekezdés f) pont] alkalmazásával végzi. Ezen jogalap alkalmazásához szükséges levezetést, valamint az ellenőrzés lefolytatásának részletes szabályait a 2. adatkezelési tájékoztató tartalmazza.

128. Az Mt. 11/A. § (3)-(4) bekezdésére figyelemmel a munkáltató az ellenőrzés során betekinthez a foglalkoztatott által a hivatali e-mail fiókban, számítástechnikai eszközön tárolt adatokba annak eldöntése érdekében, hogy az adott adat magáncélú adatnak minősül-e vagy sem.

28. Az Adatkezelő feladataival vagy tevékenységével kapcsolatba kerülő személyekre vonatkozó adatkezelések

129. Az Adatkezelő a feladataival vagy tevékenységével kapcsolatba kerülő személyek esetében elsődlegesen az alábbi adatkezeléseket végzi:

- a. az érintettek megkeresésének megválaszolásával összefüggő adatkezelés,
- b. a honlapon, közösségi oldalakon közzétett cikkekkel, írásokkal összefüggő adatkezelés,
- c. a jogi személy kapcsolattartói adatainak kezelése,
- d. természetes személy szerződéses partnerek adatainak kezelése.

29. Adatfeldolgozói tevékenység

130. Ha az adatkezelést az Adatkezelő nevében más végzi, az Adatkezelő kizárólag olyan adatfeldolgozókat vehet igénybe, akik vagy amelyek megfelelő garanciákat nyújtanak az adatkezelés a GDPR követelményeinek való megfelelését és az érintettek jogainak védelmét biztosító, megfelelő technikai és szervezési intézkedések végrehajtására.

131. Az adatfeldolgozó az Adatkezelő előzetesen írásban tett eseti vagy általános felhatalmazása nélkül további adatfeldolgozót nem vehet igénybe.

132. Az adatfeldolgozó által végzett adatkezelést az uniós jog vagy tagállami jog alapján létrejött olyan – az adatkezelés tárgyát, időtartamát, jellegét és célját, a személyes adatok típusát, az érintettek kategóriáit, valamint az adatkezelő kötelezettségeit és jogait meghatározó – szerződésnek vagy más jogi aktusnak kell szabályoznia, amely köti az adatfeldolgozót az Adatkezelővel szemben.

133. Az adatfeldolgozás érdekében kötött szerződés tartalmazza, hogy az adatfeldolgozó:

- a. a személyes adatokat kizárólag az Adatkezelő írásbeli utasításai alapján kezeli – beleértve a személyes adatoknak valamely harmadik ország vagy nemzetközi szervezet számára való továbbítását is –, kivéve akkor, ha az adatkezelést az adatfeldolgozóra alkalmazandó uniós vagy tagállami jog írja elő; ebben az esetben erről a jogi előírásról az adatfeldolgozó az adatkezelőt az adatkezelést megelőzően értesíti, kivéve, ha az adatkezelő értesítését az adott jogszabály fontos közérdekből tiltja;
- b. biztosítja azt, hogy a személyes adatok kezelésére feljogosított személyek titoktartási kötelezettséget vállalnak vagy jogszabályon alapuló megfelelő titoktartási kötelezettség alatt állnak;

- c. tiszteletben tartja a további adatfeldolgozó igénybevételére vonatkozó feltételeket;
- d. az adatkezelés jellegének figyelembevételével megfelelő technikai és szervezési intézkedésekkel a lehetséges mértékben segíti az Adatkezelőt abban, hogy teljesíteni tudja kötelezettségét az érintett jogainak gyakorlásához kapcsolódó kérelmek megválaszolása tekintetében;
- e. segíti az Adatkezelőt a kötelezettségek teljesítésében, figyelembe véve az adatkezelés jellegét és az adatfeldolgozó rendelkezésére álló információkat;
- f. az adatkezelési szolgáltatás nyújtásának befejezését követően az Adatkezelő döntése alapján minden személyes adatot töröl vagy visszajuttat az Adatkezelőnek, és törli a meglévő másolatokat, kivéve, ha az uniós vagy a tagállami jog az személyes adatok tárolását írja elő;
- g. az Adatkezelő rendelkezésére bocsát minden olyan információt, amely lehetővé teszi és elősegíti az Adatkezelő által vagy az általa megbízott más ellenőr által végzett auditokat, beleértve a helyszíni vizsgálatokat is;
- h. haladéktalanul tájékoztatja az Adatkezelőt, ha úgy véli, hogy annak valamely utasítása jogsértő.

134. Az adatfeldolgozói szerződést vagy más jogi aktust írásba kell foglalni, ideértve az elektronikus formátumot is.

135. Az adatfeldolgozó és bármely, az Adatkezelő vagy az adatfeldolgozó irányítása alatt eljáró, a személyes adatokhoz hozzáféréssel rendelkező személy ezeket az adatokat kizárólag az Adatkezelő utasításának megfelelően kezelheti, kivéve, ha az ettől való eltérésre őt uniós vagy tagállami jog kötelezi.

30. Oktatás, tájékoztatás

136. Az Adatkezelő foglalkoztatotti állományába újonnan került olyan személyeket, akik munkakörükénél fogva személyes adatokat kezelnek, az adatvédelmi tisztviselő köteles az állományba vételt követő három hónapon belül adatvédelmi oktatásban részesíteni és részére a szükséges jogszabályokat, belső normákat és egyéb segédanyagokat rendelkezésre bocsátani. Amennyiben az oktatás személyes megtartását nem indokolja valami, illetőleg az Adatkezelő nem tart rá kifejezetten igényt, az oktatás megvalósulhat előzetesen rögzített audiovizuális tartalom rendelkezésre bocsátása útján is.

137. Indokolt esetben – amennyiben az adatvédelmi tisztviselő súlyos hiányosságot észlel az Adatkezelő működése tekintetében vagy jelentős, a személyes adatok kezelését is érintő jogszabályváltozás történt – az adatvédelmi tisztviselő az Adatkezelő személyi állománya részére szánt oktatás megtartása felől intézkedik (az oktatást megalapozó fejlemények észlelését követően 2 hónapon belül), melyben tájékoztatás ad a releváns változásokról vagy az észlelt hiányosságok szempontjából indokoltá vált ismeretekről.

31. Felülvizsgálat

138. Az Adatkezelő szervezeti egységei kötelesek a nyilvántartásba vett adatkezeléseiket rendszeres időközönként, de legalább 2 évente felülvizsgálni abból a szempontból, hogy az adatkezelés céljának megvalósulásához szükséges-e a személyes adatok kezelése, valamint a GDPR és az Infotv. rendelkezéseinek megfelel-e. Törvényben elrendelt kötelező adatkezelés esetén a felülvizsgálatot az adatkezelést elrendelő jogszabályban meghatározott gyakorisággal, ennek hiányában, továbbá nem kötelező adatkezelés esetén legfeljebb háromévente, a helyben

szokásos gyakorlat szempontjából megfelelő dokumentáltság mellett el kell végezni; az erről készült feljegyzést 5 évig meg kell őrizni.

139. Ha a kötelező adatkezelés időtartamát, vagy szükségessége időszakos felülvizsgálatát törvény, helyi önkormányzat rendelete, vagy az Európai Unió kötelező jogi aktusa nem határozza meg, az Adatkezelő az adatkezelés megkezdésétől legalább háromévente felülvizsgálja, hogy az általa, valamint a megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által kezelt személyes adat kezelése az adatkezelés céljának megvalósulásához szükséges-e.

140. A NÖRI egyes adatkezeléseinek részletes leírása (adatkezelési nyilvántartás), az adatkezelési tájékoztatók, valamint az incidensvédelmi nyilvántartás 1-1 külön dokumentumban az alábbi elérési útvonalon található mappában elérhetők: \\GVVRCOMMON10\gyvrcommon10\lun07\NORISZABÁLYZATOK\HATÁLYOS_SZABÁLYZATOK_JEGYZÉKE\Adatakezesi_szabalyzat.

141. A Szabályzathoz különösen kapcsolódó, 140. pont szerinti dokumentumok új adatkezelés felmerülése, adatkezelési tájékoztató elkészítésének szükségessége vagy adatvédelmi incidens bekövetkezése esetén azonnali intézkedést igényelhetnek, ezért ezek a Szabályzat külön módosítása nélkül, a JHI által kiegészíthetők, módosíthatók, amennyiben érdemben nem hatnak ki a Szabályzatban foglalt főbb rendelkezésekre. A JHI gondoskodik arról, hogy a 140. pontban rögzítettek szerint a NÖRI szerverén a mindenkor hatályos adatvédelmi dokumentáció teljes körűen legyen elérhető.

32. Panasztételi lehetőség

142. Az Adatkezelő esetleges jogsértése ellen panasszal a NAIH-nál lehet élni:

Nemzeti Adatvédelmi és Információszabadság Hatóság
székhely: 1055 Bp., Falk Miksa utca 9-11., levelezési cím: 1363 Bp., Pf.: 9.
Telefon: +36 1 391 1400
E-mail-cím: ugyfelszolgalat@naih.hu
Web: <http://www.naih.hu>
Hivatali tárhely cím: rövid név: NAIH, KRID: 429616918

IV. fejezet Záró rendelkezések

143. Jelen szabályzat a kiadmányozása napján lép hatályba és egyidejűleg hatályát veszti a NÖRI Adatkezelési Szabályzataról szóló 26/2022 (V.31.) főigazgatói utasítása.

144. Jelen szabályzat hatályba lépésével egyidejűleg a Nemzeti Örökség Intézetének humánpolitikai eljárásrendjéről szóló Nemzeti Örökség Intézete főigazgatójának 3/2025. (I. 30.) szabályzata 23. melléklete szerinti Elszámoló lapon szereplő táblázat NÖRI Jogi és Humánpolitikai Igazgatóság sora az alábbi oszlopokkal egészül ki:

Elszámoló szervezeti egység	Az elszámolás tárgya	Megjegyzés	Dátum, aláírás
NÖRI Jogi és Humánpolitikai Igazgatóság	személyes adatok törlése a használatban volt mobiltelefon/laptop/adathordozó tekintetében	Az esetleges személyes adataim, magánjellegű tartalmaim törléséről gondoskodtam, e körben későbbi igényérvényesítési jogomról lemondok.	

Budapest, 2025. február 28.



Móczar Gábor Attila
főigazgató

Igazolom, hogy a szabályzat megfelel a szakmai előírásoknak, szempontoknak és összhangban áll a hatályos jogszabályokkal és belső szabályozókkal.

Budapest, 2025. február 28.

.....
dr. Papp-Nagy Zsuzsanna igazgató
Jogi és Humánpolitikai Igazgatóság

Nemzeti Örökség Intézete
1086 Budapest, Fiumei út 16-18.

ADATKEZELÉSI NYILVÁNTARTÁS
[NYILVÁNTARTÁS MEGNEVEZÉSE]

**A nyilvántartást kezelő szervezeti egység
megnevezése:**

A nyilvántartás megnyitásának időpontja:

A nyilvántartás lezárásának időpontja:

Az adatkezelés céljai:

Az adatkezelés jogalapja: [GDPR 6. cikk (1) bek. a)* b)* c)* d)* e)*
f)*]

Az érintettek köre: [foglalkoztatottak/egyéb]

**A személyes adatok kategóriái
(adattartalom):** [Szabályzatban felsorolt adatok közül
szükséges megjelölni]

A személyes adatok címzettjei: [Adattovábbítás esetén, pl.: adóhatóság]

**Az adatkezelési kategóriák törlésére (megőrzésére)
előírt határidők:** [jogszabály alapján]

**Az adatbiztonsági intézkedések általános
leírása:** [Szabályzat megfelelő pontjára utalás]

Kelt: Budapest, [...]

NÖRI szervezeti egység vezetője

Nemzeti Örökség Intézete
1086 Budapest, Fiumei út 16-18.

AZ ÉRINTETT TÁJÉKOZTATÁSA
AZ ADATVÉDELMI INCIDENSRŐL

Az adatvédelmi incidens jellege:

Az adatvédelmi tisztviselő/kapcsolattartó neve és elérhetősége:

Az adatvédelmi incidensből eredő, valószínűsíthető következmények:

NÖRI által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedések felsorolása:

Kelt: [...]

.....
Móczár Gábor Attila
Főigazgató

Nemzeti Örökség Intézete
1086 Budapest, Fiumei út 16-18.

JEGYZŐKÖNYV ADATVÉDELMI INCIDENSRŐL

Az adatvédelmi incidenssel érintett személyes adatok kategóriái és mennyisége:

Az adatvédelmi incidens jellege:

Az adatvédelmi incidens oka:

Az adatvédelmi tisztviselő/tájékoztatást nyújtó kapcsolattartó elérhetősége:

Az adatvédelmi incidens orvoslására/enyhítésére tett intézkedések:

Az adatvédelmi incidenssel érintettek kategóriái és száma:

Az adatvédelmi incidens helye, időpontja:

Az adatvédelmi incidens körülményei és hatásai, következményei, illetve azok súlyossága az érintettekre nézve:

Amennyiben a NÖRI mellőzte az adatvédelmi incidens bejelentést, akkor ennek oka:

Amennyiben nem volt szükséges az érintettek tájékoztatása, akkor ennek oka:

Amennyiben szükséges lett volna, de a NÖRI mellőzte az érintettek tájékoztatását, akkor ennek oka:

Az adatvédelmi incidens késedelmes bejelentésének az oka:

Az adatvédelmi incidenssel kapcsolatos egyéb adatok:

Kelt: [...]

[Jegyzőkönyv készítőjének neve, beosztása
aláírása, szervezeti egység megnevezése]