Ikt. szám: NÖRI/158-46(2020)

NEMZETI ÖRÖKSÉG INTÉZETE

Nemzeti Örökség Intézetének

Adatkezelési Szabályzata

Hatálybalépés napja: 2021. január 1.

Felülvizsgálatért felelős szervezeti egység: Jogi és Humánpolitikai Igazgatóság

A Nemzeti Örökség Intézete Főigazgatójának
46/2020. (XII.23.) Főigazgatói utasítása
a Nemzeti Örökség Intézetének Adatkezelési Szabályzatáról

A Nemzeti Örökség Intézete Adatkezelési Szabályzatát (továbbiakban: Szabályzat) 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, valamint az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény 25/A.§ (3) bekezdése alapján az alábbiak szerint határozom meg:

Preambulum

A **Nemzeti Örökség Intézete** (a továbbiakban: **Adatkezelő vagy NÖRI**) annak érdekében, hogy a munkatársaira, az ügyfeleire és más érintettekre vonatkozó jogszabályokból fakadó adatvédelmi kötelezettségeit jogszerűen és tisztességesen, valamint az érintett számára átlátható módon végezze, jelen belső szabályzatot alkotja.

1. §

A Nemzeti Örökség Intézete alapadatai, jogállása

Név: Nemzeti Örökség Intézete

Rövidített név: NÖRI

Székhely: 1086 Budapest, Fiumei út 16-18.

Jogállás: központi költségvetési szerv

Adóigazgatási szám: 15814775-2-42

PIR törzsszáma: 814779

KSH Statisztikai számjele: 15814775-8412-312-01

Képviseli: Radnainé dr. Fogarasi Katalin Főigazgató

2. §
A Szabályzat alapjául szolgáló jogszabályok

A jelen Szabályzat alapjául szolgáló jogszabályok különösen az alábbiak:

a) A természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK. rendelet hatályon kívül helyezéséről szóló Európai Parlament és a Tanács (EU) 2016/679 Rendelet Unió Általános Adatvédelmi Rendelete (GDPR rendelet)

b) Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.)
c) A közalkalmazottak jogállásáról szóló 1992. évi XXXIII. törvény
d) A munka törvénykönyvéről szóló 2012. évi I. törvény
e) A Polgári Törvénykönyvről szóló 2013. évi V. törvény
f) A Büntető Törvénykönyvről szóló 2012. évi C. törvény
g) Az általános forgalmi adóról szóló 2017. évi CXXVII. törvény
h) A számvitelről szóló 2000. évi C. törvény
i) A személyi jövedelemadóról szóló 1995. évi CXVII. törvény
j) Az adózás rendjéről szóló 2017. évi CL törvény
k) A köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről szóló 1995. évi LXVI. törvény (Levéltári tv.)
l) A pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról szóló 2017. évi LIII. törvény
m) Egyes vagyon-nyilatkozattételi kötelezettségekről szóló 2007. évi CLII. törvény
n) A személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól szóló 2005. évi CXXXIII. törvény
o) Az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény
p) A temetőkről és a temetkezésről szóló 1999. évi XLIII. törvény
q) A munkavédelemről szóló 1993. évi XCIII. törvény (Mvt.)
r) Az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény (Eüak)
s) Az egészségügyi alapellátásról szóló 2015. évi CXXIII. törvény
t) Az egyenlő bánásmódról és az esélyegyenlőség előmozdításáról szóló 2003. évi CXXV. törvény (Ebtv.)
u) A központosított informatikai és elektronikus hírközlési szolgáltatásokról szóló 309/2011. (XII. 23.) Korm. rendelet (a továbbiakban: 309/2011. Korm r.)
v) A kormányzati célú hálózatokról szóló 346/2010. (XII. 28.) Korm. rendelet (a továbbiakban: 346/2010. Korm. r.)
w) A foglalkozás-egészségügyi szolgálatról szóló 89/1995 (VII. 14.) Korm. rendelet
x) A foglalkozás-egészségügyi szolgáltatásról szóló 27/1995. (VII. 25.) NM rendelet
y) Az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezelésének egyes kérdéseiről szóló 62/1997. (XII. 21.) NM rendelet
z) A munkaköri, szakmai, illetve személyi higiénés alkalmasság orvosi vizsgálatáról és véleményezéséről szóló 33/1998. (VI. 24.) NM rendelet
aa) A központosított informatikai és elektronikus hírközlési szolgáltatásokat egyedi szolgáltatási megállapodás útján igénybe vevő szervezetekről, valamint a központi szolgáltató által üzemeltetett vagy fejlesztett informatikai rendszerekről szóló 7/2013. (II. 26.) NFM rendelet (a továbbiakban: NFM rendelet)
bb) A bírósági végrehajtásról szóló 1994. évi LIII. törvény
cc) Az üzemi balesetekkel összefüggésben a kötelező egészségbiztosítás ellátásairól szóló 1997. évi LXXXIII. törvény, valamint e törvény végrajtásáról szóló 217/1997. (XII. 1.) Korm. rendelet

3.§
Értelmező rendelkezések

Jelen Szabályzat alkalmazásában:

Adatalany/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.

Adatfeldolgozó: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő NÖRI nevében személyes adatokat kezel;

Adathordozó: Olyan fizikai eszköz, közeg, amely alkalmas adatok megőrzésére, tárolására. Az adathordozó lehet papír alapú, optikai, mágneses, elektronikus, magnetooptikai elven működő eszköz.

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;

Adatkezelés korlátozása: a tárolt személyes adatok megjelölése jövőbeli kezelésük korlátozása céljából;

Adatkezelő: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza; 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;

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;

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;

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

Érintett hozzájárulása: az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez;

Harmadik fél: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely nem azonos az érintettel, az adatkezelővel, az adatfeldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére felhatalmazást kaptak;

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

Profilalkotás: személyes adatok automatizált kezelésének bármely olyan formája, amelynek során a személyes adatokat valamely természetes személyhez fűződő bizonyos személyes jellemzők értékelésére, különösen a munkahelyi teljesítményhez, gazdasági helyzethez, egészségi állapothoz, személyes preferenciákhoz, érdeklődéshez, megbízhatósághoz, viselkedéshez, tartózkodási helyhez vagy mozgáshoz kapcsolódó jellemzők elemzésére vagy előrejelzésére használják;

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;

Vállalkozás: gazdasági tevékenységet folytató természetes vagy jogi személy, függetlenül a jogi formájától, ideértve a rendszeres gazdasági tevékenységet folytató személyegyesítő társaságokat és egyesületeket is.

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

4.§
Általános rendelkezések

1. A Szabályzat hatálya kiterjed az Adatkezelő valamennyi szervezeti egységére, továbbá az Adatkezelőnél foglalkoztatott valamennyi munkavállalóra, valamint a munkavégzésre irányuló egyéb jogviszony keretében foglalkoztatottakra, továbbá azon személyekre, akik szakmai gyakorlatukat az Adatkezelőnél töltik (a továbbiakban együttesen: foglalkoztatott).
2. A Szabályzat 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.

5.§
A személyes adatok védelmére vonatkozó általános alapelvek és szabályok

3. Az Adatkezelő által, továbbá Az Adatkezelő szervezeti egységeinél végzett adatkezelést:
   a) jogszerűen és tisztességesen, az érintett számára átlátható módon (jogszerűség, tisztességes eljárás és átláthatóság) kell végezni;
   b) a személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történhet, a céltól eltérő módon történő adatkezelés tilos (célhoz kötöttség);
   c) csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen és a cél elérésére alkalmas (adattakarékosság);
   d) az adatoknak pontosnak és szükség esetén naprakésznek kell lenniük (pontosság);
   e) az adatkezelés céljainak eléréséhez szükséges ideig szabad csak kezelni az adatokat (korlátozott tárolhatóság);

f) megfelelő technikai és szervezési intézkedésekkel biztosítani kell a személyes adatok biztonságát és védelmét (integritás és bizalmas jelleg);
g) az Adatkezelő mint adatkezelő felelős az alapelveknek való megfelelésért, továbbá képesnek kell lennie ennek bizonyítására (elszámoltathatóság).

4. Az Adatkezelő kijelenti, hogy az adatkezelése az 5. pontban foglalt alapelveknek megfelelően történik.

6.§
Az Adatkezelő vezetőjének feladat- és hatásköre, felelőssége az adatvédelem tekintetében

5. Az Adatkezelő vezetőjének feladat- és hatásköre:

a) a jogszabály által a feladat- és hatáskörébe utalt adatkezelési rendszerek egészének (nyilvántartások, adattárak, munkafolyamatok, információáramlások és feldolgozások, jogosultságok) kialakíttatása és irányítása, rendeltetésszerű működtetése, időszakos felülvizsgálata;
b) a személyes adatok megfelelő biztonságának biztosítása érdekében az adatkezelések szervezeti és működési feltételeinek kialakítása, a működési és az adatbiztonsági követelmények érvényre juttatásának biztosítása;
c) az érintettek jogai érvényesülésének biztosítása érdekében az érintettek megfelelő tájékoztatására, valamint az érintetti kérelmek határidőben történő elbírálására alkalmas eljárásrend kialakítása;
d) az adatvédelmi és adatbiztonsági szabályok gyakorlati érvényesülésének ellenőrzése, intézkedés a hiányosságok felszámolására.

7.§
Az Adatkezelő adatvédelmi tisztviselője

6. Az Adatkezelőnél az adatvédelmi tisztviselői feladatokat – megbízási jogviszony alapján – külső szakértő látja el.

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

8. 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 együtt gondoskodik a belső adatvédelmi és adatbiztonsági szabályzat folyamatos aktualizálásáról;
f) a Jogi és Humánpolitikai Igazgatósággal együttműködve gondoskodik az adatvédelmi nyilvántartás és az adatvédelmi incidensek nyilvántartásának vezetéséről;

g) adatvédelmi incidens bekövetkezése esetén haladéktalanul intézkedik annak kezelésére, valamint szükség esetén ellátja a Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: NAIH) részére történő bejelentéssel, valamint az érintett tájékoztatásával kapcsolatos feladatokat; indokolt esetben büntető-, szabálysértési, fegyelmi eljárást vagy egyéb felelősségre vonást kezdeményez;
h) a feladatkörébe tartozó bejelentéseket kivizsgálja, valamint kivizsgálásra továbbítja az illetékes adatkezelő szerv vezetőjének, valamint ellenőrzi a bejelentés tárgyában tett intézkedést;
i) kapcsolatot tart a NAIH-al és az érintettekkel, más szervekkel;
j) a Jogi és Humánpolitikai Igazgatósággal együttműködve nyilvántartást vezet az Adatkezelő vonatkozásában az elutasított közérdekű adatigénylések számáról és az elutasítások indokairól, és minden év január 31-ig tájékoztatja a NAIH-t az elutasított kérelmekről, valamint az elutasítások indokairól;
k) bejelenti a NAIH részére az adatvédelmi tisztviselő adatait (név, postai és elektronikus levélcím) és azok változását, továbbá gondoskodik ezen adatok Adatkezelő honlapján történő közzétételéről;
l) a Jogi és Humánpolitikai Igazgatósággal együttműködve állásfoglalást ad az Adatkezelő szervezeti egységei részére az adatok nyilvánossága, megismerhetősége tárgyában;
m) ellátja a külön jogszabályban meghatározott feladatait;
n) 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;
o) közreműködik Jogi és Humánpolitikai Igazgatósággal és a kérelem tárgyában érintett szakterülettel az érintett hozzáférési joga gyakorlására vonatkozó kérelmére;
p) a beérkezett közérdekű adatigénylésekre – a Jogi és Humánpolitikai Igazgatósággal együttműködve – elkészíti a választervezetet az Infotv. által előírt határidőben;
q) ellátja mindazon feladatokat, amelyeket a hatályos adatvédelmi jogszabályok és a megbízási szerződés részére feladatként meghatároz.

9. 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 betekinthet, amely Az Adatkezelő adatkezelési tevékenységével összefügg.

10. 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.

11. Az Adatkezelő adatvédelmi tisztviselőjének elérhetőségét Az Adatkezelő honlapon közzétett adatvédelmi tájékoztatója tartalmazza.

8.§
Az Adatkezelő által vezetett nyilvántartások és az adatvédelmi nyilvántartás

12. Az Adatkezelő által kezelt, személyes adatot tartalmazó adatkezelések nyilvántartásba vételét az érintett szervezeti egység az 1. számú melléklet szerinti adatlap Jogi és Humánpolitikai Igazgatóság részére történő megküldésével kezdeményezi az adatvédelmi tisztviselőnél.

13. Az érintett szervezeti egység köteles gondoskodni az általa kezelt személyes adatok vonatkozásában az adatvédelmi adatlap évenkénti felülvizsgálatáról, valamint szükség szerinti aktualizálásáról. Az aktualizált adatlapot haladéktalanul továbbítani köteles a Jogi és Humánpolitikai Igazgatóság részére.

14. Az Adatkezelő adatvédelmi nyilvántartását a Szabályzat 3. számú melléklete tartalmazza.

15. Ha Az Adatkezelő által kezelt nyilvántartásból betekintésre nem jogosult személy kíván személyes adatokat megismerni, a betekintéshez engedélyt kell kérnie, amelyet a Főigazgató ad ki. Az ilyen jellegű betekintésekről betekintési nyilvántartást kell vezetni (2. számú melléklet), amelyben rögzíteni kell:
    a) betekintést/másolatot kérő neve, rendelkezésre álló azonosító adatai
    b) a betekintés jogalapja;
    c) kérelem kelte;
    d) betekintés/másolat tárgya;
    e) a kérelem teljesítésének időpontja;
    f) a betekintés korlátozásának vagy elutasításának indoka.

16. Az Adatkezelő az általa kezelt adatokkal összefüggésben felmerült adatvédelmi incidensekről a 4. számú melléklet szerinti jegyzőkönyvekből álló nyilvántartást vezet, mely 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.).

17. Ha az Adatkezelő a NAIH adatvédelmi hatósági eljárásban hozott határozatát nem fogadja el, adatvédelmi hatósági eljárás esetén az adatvédelmi tisztviselő egyetértésének kikérését követően a bírósági felülvizsgálat kezdeményezésére nyitva álló határidőn belül a bírósághoz fordulhat.

9.§
Az adatvédelmi hatásvizsgálat

18. Valamennyi új, vagy a korábbiaktól eltérő adatkezelést előíró vagy eredményező jogszabály vagy belső szabályozó eszköz, eljárásrend, eszköz vagy technológia bevezetését vagy változását megelőzően, az előkészítés során az adatvédelmi tisztviselő megvizsgálja, hogy a tervezett adatkezelésnek várhatóan milyen hatásai lesznek az érintettek alapvető jogai érvényesülésére (a továbbiakban: előzetes kockázatbecslés).

19. Az előzetes kockázatbecslés során az adatvédelmi tisztviselő az általános adatvédelmi rendelet, valamint az Infotv. rendelkezései alapján, a NAIH iránymutatásai figyelembevételével, szükség esetén az érintett szakterületek véleményének kikérésével vagy

bevonásával azonosítja a tervezett adatkezeléssel járó várható kockázatokat az érintettek alapvető jogai érvényesülése vonatkozásában. Az adatvédelmi tisztviselő az előzetes kockázatbecslés eredményét írásban rögzíti.

20. Nem szükséges adatvédelmi hatásvizsgálatot lefolytatni, amennyiben az adatvédelmi tisztviselő megállapítja, hogy:

    a) az előzetes kockázatbecslés alapján a tervezett adatkezelés valószínűsíthetően nem jár magas kockázattal;
    b) a tervezett adatkezelés a NAIH által meghatározott kivételi körbe tartozik;
    c) a tervezett adatkezeléssel megegyező adatkezelés esetében korábban lefolytatott adatvédelmi hatásvizsgálat eredménye rendelkezésre áll, vagy
    d) a jogszabályban előírt adatkezelés esetében a jogalkotó lefolytatta előzetesen a hatásvizsgálatot.

21. Az adatvédelmi hatásvizsgálat lefolytatásáról vagy mellőzéséről az adatvédelmi tisztviselő által tett megállapítások figyelembevételével Az Adatkezelő vezetője dönt.

22. Az adatvédelmi hatásvizsgálat lefolytatásának mellőzése esetén annak indokait az adatvédelmi tisztviselő írásban rögzíti és az előzetes kockázatbecslés irataihoz csatolja.

23. Az adatvédelmi hatásvizsgálat lefolytatása során a GDPR, valamint az Infotv. rendelkezései alapján, a NAIH iránymutatásai figyelembevételével az arra kijelölt csoport a NAIH honlapjáról letölthető adatvédelmi hatásvizsgálati szoftver („PIA software") alkalmazásával történik.

24. Adatvédelmi hatásvizsgálatot kell elvégezni különösen akkor, ha:
    a) Az Adatkezelő olyan adatkezelést végez, amely az érintettek módszeres és kiterjedt értékelésére épül, és amely adatkezelés alapján az érintettre nézve joghatással bíró vagy más hasonló jelentős döntést hoznak,
    b) Az Adatkezelő a mindenki számára korlátozás nélkül igénybe vehető területen kamerás megfigyelést alkalmaz,
    c) Az Adatkezelő által végzett adatkezelés szerepel a NAIH által, az adatvédelmi hatásvizsgálat elvégzésével összefüggésben nyilvánosságra hozott jegyzékben.

25. Az adatvédelmi hatásvizsgálatnak ki kell terjednie legalább:
    a) a tervezett adatkezelés módszeres leírására és az adatkezelés céljainak ismertetésére, beleértve adott esetben az adatkezelő által érvényesíteni kívánt jogos érdeket,
    b) az irányadó jog vonatkozó rendelkezésire, valamint - amennyiben lehetséges - a NAIH vagy bíróságok gyakorlatára, a kialakult gyakorlatra,
    c) az adatkezelés céljaira figyelemmel az adatkezelési műveletek szükségességi és arányossági vizsgálatára,
    d) az érintett jogait érintő kockázatok vizsgálatára és a kockázatok kezelését célzó intézkedések bemutatására.

26. Amennyiben az Adatkezelő által feltérképezett kockázatok mérséklését követően továbbra is magas kockázatúnak tekinthető az adatkezelés, akkor előzetes konzultáció kérelmével a NAIH-hoz kell fordulni.

27. Az adatvédelmi hatásvizsgálatot az adatvédelmi tisztviselő végzi el, és annak eredményét a Főigazgató hagyja jóvá. A Főigazgató dönt arról is, hogy szükséges-e előzetes konzultáció érdekében a NAIH-hoz fordulni.

10.§
Előzetes tájékoztatás kötelezettsége

28. Az Adatkezelőnek valamennyi adatkezeléséről tájékoztatni kell az érintetteket. Amennyiben az Adatkezelő előzetesen nem tájékoztatja az adatkezelésről az érintetteket, az adatkezelés nem végezhető.

29. Az Adatkezelő a tájékoztatási kötelezettségét az érintettek és a munkavállalók tájékoztatása céljából elkészített adatkezelési tájékoztatók megalkotásával és nyilvánosságra hozatalával vagy közlésével teljesíti. Kivételesen elfogadható az is, ha az Adatkezelő valamely adatkezeléshez kapcsolódóan eseti tájékoztatást ad át az érintetteknek.

30. Amennyiben az Adatkezelő a személyes adatokat az érintettől veszi fel (ilyennek minősül az érintett által a honlapon megadott adatok vagy a munkavállaló 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, ha adatvédelmi tisztviselőt nevez ki, akkor annak elérhetőségei,
    b) az adatkezelés célja, jogalapja, illetve a személyes adatok tárolásának időtartama, vagy ha ez nem lehetséges, akkor ezen időtartam meghatározásának szempontjai,
    c) az érdekmérlegelés jogalapjának alkalmazása esetén az adatkezelő vagy harmadik fél jogos érdekei,
    d) a személyes adatok címzettjei, vagy a címzettek kategóriái,
    e) az érintettet megillető jogok, illetve a NAIH-hoz fordulás lehetősége,
    f) a hozzájárulás bármely időpontban való visszavonásához való jog, illetve az arra vonatkozó tájékoztatás, hogy ez nem érinti a visszavonás előtt a hozzájárulás alapján végrehajtott adatkezelés jogszerűségét,
    g) a személyes adatok megadása jogszabályon alapul, vagy szerződés kötésének előfeltétele, valamint, hogy az érintett köteles-e a személyes adatokat megadni, továbbá, hogy milyen lehetséges következményeikkel járhat az adatszolgáltatás elmaradása.

31. Amennyiben az Adatkezelő a személyes adatokat nem az érintettől veszi fel, hanem más forrásból szerzi meg (ilyennek minősül amennyiben az érintett adatát továbbítják Az Adatkezelő számára), akkor az adatkezelési tájékoztatónak ki kell terjednie:
    a) a szabályzat 30. pontjában foglaltakra és
    b) a személyes adatok forrására.

32. Az adatkezelési tájékoztatónak tömörnek kell lennie. Amennyiben az adatkezelési tájékoztató terjedelmes, hosszabb dokumentum, akkor az Adatkezelőnek a tájékoztatóból készítenie kell egy rövidebb változatot. Ebben az alábbi adatokat kell feltüntetni: az adatkezelő neve, elérhetőségei, az adatkezelés célja, jogalapja, illetve a személyes adatok tárolásának időtartama, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjai, az érdekmérlegelés jogalapjának alkalmazása esetén az adatkezelő vagy harmadik fél jogos érdekei. A rövidebb változatban utalni kell a teljeskörű tájékoztatás elérhetőségére.

33. Az adatkezelési tájékoztatónak átláthatónak kell lenni. A tájékoztatót bekezdésekre kell tagolni, és ahol szükséges, felsorolást kell alkalmazni a szöveg könnyebb áttekinthetősége, olvashatósága érdekében.

34. 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 munkavállalókat érintő adatkezelési tájékoztatót a helyben szokásos és általában ismert módon közzé kell tenni, így ki kell függeszteni a hirdetőbálára és továbbítani kell a belső levelezőrendszeren keresztül.

35. Az Adatkezelő a jelen Szabályzat mellékletét képző adatkezelési tájékoztatókat köteles az érintettek rendelkezésére bocsátani.

36. Az adatkezelési tájékoztatót közérthetően kell megfogalmazni. Az adatkezelési tájékoztatóban kerülni kell a jogszabály szó szerinti megismétlését, és törekedni kell az egyszerű, világos megfogalmazásra. A tájékoztatónak rövidebb mondatokból kell állnia, kerülni kell a több tagmondatból álló összetett mondatok alkalmazását.

11.§
Érintetti Joggyakorlás

11.1. A feladatok megoszlása az érintetti joggyakorlás során

37. Az érintett által benyújtott valamely jogának gyakorlására irányuló kérelem elbírálása és megválaszolása az Adatkezelő kérelemmel érintett adatkezelést végző szervezeti egységének feladata. A kérelem elbírálásába és megválaszolásába a Jogi és Humánpolitikai Igazgatóságot és az Adatkezelő adatvédelmi tisztviselőjét kötelesek bevonni.

38. Az a szervezeti egység, amelyhez a kérelem benyújtásra került, köteles a kérelmet 3 munkanapon belül a Jogi és Humánpolitikai Igazgatóság részére megküldeni, amely azt haladéktalanul továbbítja Az Adatkezelő adatvédelmi tisztviselője részére.

39. Az adatvédelmi tisztviselő feladata az érintettnek küldendő válaszlevél tervezetének a kialakítása, illetve annak teljesítésével kapcsolatos feladatok ellátása (például másolat kéréshez való jog gyakorlása estén a dokumentum másolása vagy a kamera felvételek anonimizálása érdekében árajánlat kérése). Az adatvédelmi tisztviselő kérésére más munkavállalóknak vagy az IT területen szakmai kompetenciával rendelkező közre kell működniük a feladatok ellátásában, a tervezet kialakításában. Az adatvédelmi tisztviselő által elkészített tervezetet az a Jogi és Humánpolitikai Igazgatósága véleményezi.

40. A tervezet be kell mutatni a Főigazgató számára. Az érintetti kérelem megválaszolását a Főigazgató vagy az általa kijelölt vezetőnek kell kiadmányoznia.

11.2. Hozzáféréshez való jog

41. Amennyiben az érintett 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) milyen adatkezelések vannak az érintett vonatkozásában, és az adatkezeléseknek mi a célja és a jogalapja;
    c) az adatkezelésnek mi az időtartama, illetve ezen időtartam meghatározásának szempontjai;
    d) kiknek továbbítja a személyes adatokat az adatkezelő;

e) az érintettet az adatkezeléssel összefüggésben megillető jogokról;
f) amennyiben nem az érintettől vették fel a személyes adatokat, akkor azok forrásáról;
g) a NAIH-nak címzett panasz benyújtásának jogáról.

42. 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.

11.3. Másolatkéréshez való jog

43. 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.

44. A másolat kéréséhez való jogot:
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
c) kell teljesíteni.

45. 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.

11.4. Helyesbítéshez való jog

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

47. Az érintett kérelme akkor teljesíthető, ha abban megjelölte, hogy mely személyes adat módosítását kéri és mi a helyes személyes adata.

11.5. Törléshez való jog

48. Az Adatkezelőnek a személyes adatokat törölnie kell, amennyiben
a) megszűnt az adatkezelés célja,
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.

49. 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 a 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.

11.6. Elfeledtetéshez való jog

50. Amennyiben az Adatkezelő a személyes adatokat nyilvánosságra hozta, és a belső adatkezelési szabályzat 48. pontja 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.

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

52. Amennyiben az Adatkezelő a saját honlapján hozta nyilvánosságra a személyese adatokat, akkor azokat onnan el kell távolítani.

53. 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.

54. 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.

55. Az 49. pontban szereplő kivételeket az elfeledtetéshez való jog gyakorlása esetén szintén alkalmazni kell.

11.7. Korlátozáshoz való jog

56. 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.

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

58. 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) kimenti, 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.

59. 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) kimenti, 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.

60. 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.

61. 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.

62. Ha az érintett kérelme megalapozott, akkor az Adatkezelő törli a személyes adatot.

11.8. Adathordozhatósághoz való jog

63. 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.

64. 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.

65. Az Adatkezelőnek a 63. 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) kimenti (a külső adathordozót az érintett is biztosíthatja).

11.9. A tiltakozás joga

66. Az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból bármikor tiltakozzon személyes adatainak az érdekmérlegelés jogalapjának alkalmazásával történő kezelése ellen.

67. Tiltakozás esetén meg kell vizsgálni azt, hogy az érintett által megjelölt adatkezelés esetében az érintett által hivatkozott tények, érvek miatt a Adatkezelőnek van-e lehetősége arra, hogy a személyes adatokat törölje, vagy az adatkezelést az érintett vonatkozásában megszüntesse.

68. 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.

11.10. Az érintett azonosítása

69. Ha az Adatkezelőnek 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 nyújtsa be a kérelmét,
    c) az érintett az Adatkezelő székhelyén bemutatja valamely személyazonosító igazolványát (személyi igazolvány, jogosítvány, útlevél).

70. 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.

11.11. A kérelem teljesítésének határideje

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

72. 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.

11.12. Az érintetti kérelem teljesítése

73. Az Adatkezelő nem teljesíti az érintett kérelmét, ha azt telefonhívás útján, szóban közli. Az érintett elektronikus úton vagy papír alapon küldött kérelme teljesíthető. Erre az érintettet a telefonhívás során tájékoztatni kell.

74. Az Adatkezelőnek olyan módon kell teljesíteni az érintett kérelmét, amilyen formátumban az érintett kéri.

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

76. Ha az érintett a kérelmében nem jelölte meg, hogy milyen formátumban kéri a másolatot, akkor az Adatkezelőnek fel kell vennie az érintettel a kapcsolatot, és tisztázni kell, hogy milyen formátumban szeretné, ha az Adatkezelő teljesítené a kérelmét. A kapcsolatfelvételnek elsődlegesen telefonhívás vagy elektronikus levelezés útján kell megtörténnie, ha nincs ilyen, akkor postai úton kell felvenni a kapcsolatot az érintettel.

77. 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 is akar az érintett gyakorolni, akkor ennek tisztázása érdekében fel kell venni a kapcsolatot.

78. 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 a Adatkezelő, másrészt pedig végre kell hajtani a személyes adatok törlését - ha nem áll fenn valamely kivétel - és erről az érintettet tájékoztatni kell).

79. Az értintett kérelmének teljesítését díjmentesen kell biztosítani.

11.13. Az érintetti kérelem megtagadása

80. 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.

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

82. Az érintett kérelmének megtagadásáért nem lehet díjat felszámítani.

83. 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 tagadhatja meg a kérelem teljesítést), valamint arról, hogy

b) az érintett panaszt nyújthat be valamely felügyeleti hatóságnál, és élhet bírósági jogorvoslati jogával.

12.§
Az adatvédelmi incidensek kezelése

84. 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. Adatvédelmi incidensnek minősül többek között az alábbiak:

- harmadik fél által a személyes adatokat tároló informatikai rendszer vagy adatkezelő szoftverhez történő jogosulatlan hozzáférés,
- a személyes adatok jogosulatlan titkosítása, amelynek következtében a személyes adatokhoz - akár átmenetileg - nem lehet hozzáférni vagy az Adatkezelő adatkezelései során felhasználni,
- ha az Adatkezelő munkavállalója jogosulatlanul hozzáfér személyes adatokhoz, vagy a jogosultsági szintjét meghaladóan fér hozzá a személyes adatokhoz, vagy a munkavállaló által jogosulatlanul végrehajtott adatkezelési művelet (például a személyes adatokat tartalmazó adatbázis kimentése külső adathordozóra),
- személyes adatok vétlen vagy szándékos, felhatalmazás nélküli nyilvánosságra hozatala,
- személyes adatokat tartalmazó dokumentum más számára történő hozzáférhetővé tétele,
- személyes adatokat tartalmazó postai küldemény téves címzetthez történő elpostázása,
- személyes adatokat tartalmazó e-mail téves címzettnek történő kiküldése,
- személyes adatokat tartalmazó adathordozó vagy informatikai eszköz elvesztése,
- a személyes adatokat tároló informatikai eszköz vagy az ilyen adatokat tartalmazó dokumentumok sérülése, megsemmisülése (ideértve a tűzesetet vagy a vízkár által okozott sérülést vagy megsemmisülést), amelynek következtében a személyes adatokhoz - akár átmenetileg - nem lehet hozzáférni vagy az Adatkezelő adatkezelései során felhasználni.

85. Az adatvédelmi incidenseknek alapvetően három kategóriája különböztethető meg:

a) bizalmassági incidens;
b) sértetlenséggel kapcsolatos incidens és
c) hozzáférhetőséggel kapcsolatos incidens.

86. 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.

87. Adatvédelmi incidens bekövetkezése esetében a következő lépéseket kell a Adatkezelőnek, mint adatkezelőnek megtennie:

a) az adatvédelmi incidens kockázati besorolásának elvégzése;
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.

88. 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;
f) az Adatkezelő mint adatkezelő sajátosságai.

89. Az Adatkezelőnél adatvédelmi incidens bekövetkezésének észlelése esetén haladéktalanul jelentést kell tenni a Jogi és Humánpolitikai Igazgatóság vezetőjének, aki soron kívül értesíti az adatvédelmi tisztviselőt és a Főigazgatót.

90. Adatvédelmi incidensre vonatkozó értesítést követően haladéktalanul fel kell függeszteni azt az adatkezelést, amit az adatvédelmi incidens érintett.

91. A felfüggesztés megszüntethető különösen, ha
    - a rendelkezésre álló információk alapján az adatvédelmi incidensnek nincsenek és nem is várhatóak súlyos következményei, vagy
    - a felfüggesztést követően az Adatkezelő olyan intézkedéseket hozott, amelyek biztosítják, hogy az adatvédelmi incidensnek nincsenek és nem is várhatóak súlyos következményei.

92. A felfüggesztés megszüntetéséről az adatvédelmi tisztivelő és a Jogi és Humánpolitikai Igazgatóság vezetőjének javaslatára a Főigazgató dönt. A javaslatban ki kell térni arra, hogy
    - milyen adatvédelmi incidens történt (a személyes adatok típusa, mennyisége, érintettek száma, kategóriái, milyen következményei voltak vagy lehettek volna az érintettre),
    - miért javasolja a felfüggesztés megszüntetését.

93. Az adatvédelmi tisztviselő haladéktalanul tájékozódik a bekövetkezett adatvédelmi incidens körülményeiről, felméri, hogy a 87. pontban meghatározott szempontok alapján az incidens valószínűsíthetően kockázatot eredményez-e az érintettek jogai érvényesülése vonatkozásában, és a 88. és 90. pontok alapján megteszi a szükséges lépéseket a mielőbbi károk elhárítása érdekében.

94. Amennyiben az adatvédelmi tisztviselő által elvégzett 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 megteszi a bejelentést, ezzel egyidejűleg jelentést tesz a Főigazgató és a Jogi és Humánpolitikai Igazgatósága 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.

95. 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 vizsgálatban fel kell térképezni, hogy
    - mi volt az adott esemény oka,
    - miért nem következett be adatvédelmi incidens, illetve
    - amennyiben az adott esemény kapcsán értelmezhető - hogyan lehet megelőzni azt, hogy a jövőben ne következzen be hasonló esemény.

96. Abban az esetben, ha bizonyítottan adatvédelmi incidens történt, azonban arról történő tudomásszerzés időpontjában vagy az előzetes vizsgálat alapján megállapítható, hogy az incidensnek valószínűsíthetően nincs kockázata az érintettekre 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 Jogi és Humánpolitikai Igazgatósága javaslata alapján a Főigazgató dönt. A javaslatban ki kell térni arra, hogy

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

Amennyiben a Főigazgató a javaslatot elfogadja, akkor az adatvédelmi incidenst fel kell vezetni az incidens-nyilvántartásba.

97. Az adatvédelmi incidensről való tudomásszerzésnek az tekinthető, ha a kockázatelemzés alapján a NÖRI mint adatkezelő ésszerű mértékű bizonyosságot szerez arról, hogy biztonsági esemény történt, amely a személyes adatokkal kapcsolatos jogellenes műveletekhez vezet. Tudomásszerzésnek minősülnek különöse az alábbiak:
    - az adatvédelmi incidens bekövetkezésére utaló körülményt az Adatkezelő munkavállalója fedezi fel,
    - 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),
    - az Adatkezelőt telefonon keresztül adatvédelmi incidens bekövetkezésére utaló körülményről értesítik (abban az esetben is, ha a hívó fél ismeretlen vagy névtelen),
    - a sajtóban vagy más honlapon megjelent, adatvédelmi incidens bekövetkezésére utaló körülmény, amelyről az Adatkezelőt értesül vagy arról értesítik,
    - az Adatkezelő által megbízott adatfeldolgozó e-mailben vagy telefonon jelzi, hogy az Adatkezelő által kezelt személyes adatokkal összefüggésben adatvédelmi incidens következett be.

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

99. 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 (5. számú melléklet).

100. 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.

101. Az adatvédelmi incidens kezelésére az Adatkezelőn belül, ad hoc jelleggel incidenskezelő csoport működik, amelynek tagja egy informatikai szakember, egy kommunikációs szakember, egy jogász és az adatvédelmi tisztviselő. Az incidenskezelő csoportban az adatvédelmi tisztviselő a koordinációért és a kapcsolattartásért felelős személy.

102. Ha az adatvédelmi incidens olyan súlyú és volumenű, külső szakértők bevonására is lehetőség van.

103. Az Adatkezelő által megbízott adatfeldolgozó az adatvédelmi incidenst az arról való tudomásszerzést követően, indokolatlan késedelem nélkül köteles az Adatkezelő részére bejelenteni.

104. A NÖRI mint adatkezelő az adatvédelmi incidensekről nyilvántartást vezet, feltüntetve abban az adatvédelmi incidensekhez kapcsolódó tényeket, annak hatásait és az orvoslásukra tett intézkedéseket.

13.§
Adatbiztonsági intézkedések

105. 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.

106. Az Adatkezelőnél bármely foglalkoztatási jogviszonyban lévő személyek kötelesek jelen szabályzat, továbbá a hatályos jogszabályok szerint a rájuk bízott, valamint tudomásukra jutott személyes adatokat és üzleti titkokat időbeli korlátozás nélkül megőrizni. A munkavállalók 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.

107. Minden személyes adatot, üzleti titkot tartalmazó rendszerhez való hozzáférésre feljogosított foglalkoztatott köteles titoktartási kötelezettségvállalást tenni. A kötelezettségvállalásban 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.

108. 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 tartani. Az asztalon és az irodában egyéb helyen hivatalos iratok csak a munkavégzés céljából és annak időtartama alatt tárolhatók.

109. A fenti bekezdésben felsorolt iratok elzárásáért az a foglalkoztatott felelős, akinél azok a munkaidő befejezésekor találhatók. Azokat a helyiségeket, ahol közös használatú nyomtató, fénymásológép, szkenner, 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 eszközből. Az irodatechnikai eszközben maradt iratért adatvédelmi szempontból az felel, aki az iratot az irodatechnikai eszközzel fizikailag előállította, valamint módosította.

110. 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.

111. Személyes adatokat is tartalmazó iratot Az Adatkezelő székhelyéről kivinni – munkaköri feladat ellátásának kivételével – csak az érintett szervezeti egység vezető 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.

112. Iratok és adatok mobiltelefonon, valamint egyéb elektronikus úton 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.

113. Az egyes nyilvántartások, adatkezelések tekintetében a hozzáférési jogosultságot a Főigazgató és a szervezeti egységek vezetőinek kell meghatároznia és az időszerű állapotnak megfelelő nyilvántartásukról gondoskodnia.

114. 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.

115. Az egyes adatkezelésekhez a hozzáférési jogosultságot személyre szólóan kell megállapítani, a jogosultságot az érintett munkaköri leírásában is rögzíteni kell. Amennyiben a jogosultság megállapítására alapot adó körülményben változás történik, haladéktalanul intézkedni kell a jogosultság módosítására vagy visszavonására.

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

117. A kezelt adatokat úgy kell tárolni, hogy azokhoz illetéktelenek ne férhessenek hozzá. Papír alapú adathordozók esetében a fizikai tárolás, irattárazás rendjének kialakításával, elektronikus formában kezelt adatok esetén központi jogosultságkezelő rendszer alkalmazásával szükséges megoldani a tárolást.

118. 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.

119. A papír alapú adathordozókat iratmegsemmisítő segítségével, vagy 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.

120. A papír alapon kezelt személyes adatok biztonsága érdekében Az Adatkezelő az alábbi intézkedéseket alkalmazza (fizikai védelem):

a) a dokumentumokat biztonságos, jól zárható száraz helyiségben kell elhelyezni;
b) Az Adatkezelő épülete és helyiségei tűzvédelmi és vagyonvédelmi berendezéssel vannak ellátva;
c) a személyes adatokat csak az arra jogosult személyek ismerhetik meg, azokhoz harmadik személyek nem férhetnek hozzá;
d) Az Adatkezelő adatkezelést végző munkatársa a munkavégzése során csak úgy hagyhatja el azt a helyiséget, ahol adatkezelés folyik, hogy a rá bízott adathordozókat elzárja, vagy az adott helyiséget bezárja.

121. Amennyiben a papíralapon kezelt személyes adatok digitalizálására kerül sor, akkor a digitálisan tárolt dokumentumokra irányadó szabályokat kell alkalmazni.

122. A papír alapú dokumentumok megsemmisítésére iratmegsemmisítőt kell használni.

123. Az Adatkezelő Biztonsági Szabályzatában a fentieken túl meghatározott intézkedések biztosítják a megfelelő technikai és fizikai védelmet a személyes adatok számára. Az Adatkezelő által elektronikusan vagy papír alapon kezelt összes személyes adat az intézet székhelyén található zárt objektumaiban található, amelyek állandó 24 órás élőerős őrzés alatt állnak. A Biztonsági Szabályzat részletesen rendelkezik arról, hogy az egyes munkavállalók, csak a munkakörük elvégzéséhez szükséges helyiségekbe juthassanak be. A személyes adatok védelme érdekében az épületekbe való belépési jogosultságokat központi adminisztrált kulcskiadással, valamint mágneskártyás beléptetési rendszerrel kontrollálja az Adatkezelő Szolgáltatási Igazgatósága. Az Adatkezelő papír alapú iratforgalmának biztonságát a NÖRI Iratkezelési Szabályzatának rendelkezései biztosítják. Az Adatkezelő székhelyén működő irattár és iktatási rendszer elkülönített objektumban riasztóval védett helyiségben található.

124. Informatikai védelem:

a) az adatkezelés során használt számítógépek és mobil eszközök (egyéb adathordozók) az Adatkezelő tulajdonát képezik;
b) a számítógépeken található adatokhoz személyre generált és kiadott felhasználónévvel és jelszóval lehet csak hozzáférni;

c) a központi szerver géphez csak megfelelő jogosultsággal és csakis az arra kijelölt személyek férhetnek hozzá;
d) a digitálisan tárolt adatok biztonsága érdekében az Adatkezelő adatmentéseket és archiválásokat alkalmaz;
e) az Adatkezelő által használt személyes adatokat tartalmazó számítógépes rendszer vírusvédelemmel és tűzfallal van ellátva.
f) az adatok továbbítása titkosított csatornán történik.
g) A központosított informatikai és elektronikus hírközlési szolgáltatásokat egyedi szolgáltatási megállapodás útján igénybe vevő szervezetekről, valamint a központi szolgáltató által üzemeltetett vagy fejlesztett informatikai rendszerekről szóló 7/2013. (II. 26.) NFM rendelet értelmében a NÖRI teljes informatikai infrastruktúráját a NISZ üzemelteti, mint szolgáltató, így az informatikai biztonsági intézkedések a NISZ vonatkozó szabályzata alapján kötelező érvényűek, melyek megfelelnek a GDPR előírásainak.

14.§
A munkáltatói adatkezelésekre vonatkozó közös szabályok

125. 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.

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

127. A foglalkoztatott kötelezhető 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

128. A fentiektől eltérően személyes adatokat igazoló okiratról történő másolatkészítésre kizárólag jogszabály felhatalmazása alapján kerülhet sor.

129. 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.

15.§
A munkavállalókra, illetve a közalkalmazottakra vonatkozó adatkezelések

130. Az Adatkezelő elsődlegesen az alábbi munkavállalókat érintő adatkezeléseket végzi:
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 munkavállalói nyilatkozatokkal összefüggő adatkezelés,
i) a foglalkoztatott magáncélú elérhetőségek kezelésével összefüggő adatkezelés,
j) az NÖRI nevében történő kapcsolattartással összefüggő adatkezelés,
k) az utazások megszervezésével összefüggő adatkezelés,
l) a vagyonnyilatkozat-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.

131. Amennyiben a Szabályzat (ideértve a 3. számú mellékletben található adatkezelési nyilvántartást is) 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,
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 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).

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

133. 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 vagyonnyilatkozat-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

134. A munkáltatói adatkezelések körülményeit részletesen a 3. számú mellékletben található adatkezelési nyilvántartás tartalmazza.

16.§

A hivatali email fiók, számítástechnikai eszköz és internet használatának, illetve az otthoni munkavégzés szabályai, valamint a munkáltatói ellenőrzés keretei

135. 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 keresztnevét tartalmazó email címet és ehhez tartozó e-mail fiókot bocsát rendelkezésre (a továbbiakban: hivatali email fiók). A hivatali email 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.

136. 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. 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 a magáncélú adatokat haladéktalanul törölniük kell.

137. 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).

138. Az Adatkezelő magánhasználat tilalmától való eltérést vagy saját számítástechnikai eszközt használatát csak külön a 7. számú melléklet szerinti nyilatkozattétel után, az alábbiakban ismertetett módon engedélyezi, amelyet a foglalkoztatott nyilatkozatban megerősíti, akkor is csak olyan formában, hogy a hivatali munkavégzést ne akadályozza.

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

a) a munkavállalónak kell biztosítania a részére átadott munkaeszközök (laptop, mobiltelefon, USB) biztonságos szállítását és tárolását,

b) a munkavállalónak 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 munkavállalónak 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 munkavállaló köteles gondoskodni a nála lévő munkaeszközök és a munkáltatói hivatalos iratok elzárásáról;
e) illetéktelen használat észlelése esetén a munkavállaló köteles haladéktalanul felvenni a kapcsolatot Az Adatkezelő informatikai szakemberével.

140. Az Adatkezelőnek a Mt. 11/A. § (1) bekezdésében biztosított jogszabályi felhatalmazás alapján lehetősége van annak ellenőrzésére, hogy
a) a foglalkoztatottak megtartották-e a magáncélú használat tilalmára vonatkozó kötelezettségüket,
b) a felhasználók megtartották a titoktartási kötelezettségüket.

141. Az Adatkezelő az ellenőrzéssel együtt járó adatkezelését az érdekmérlegelés jogalapjának [GDPR 6. cikk (1) bekezdés f) pont] alkalmazásával végzi. Ezen jogalap alkalmazásához szükséges levezetést, valamint az ellenőrzés lefolytatásának részletes szabályait a jelen Szabályzat 8. számú melléklete tartalmazza.

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

17.§
Az Adatkezelő feladataival vagy tevékenységével kapcsolatba kerülő személyekre vonatkozó adatkezelések

143. 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.

144. A fenti adatkezelések körülményeit részletesen a 3. számú mellékletben található adatkezelési nyilvántartás tartalmazza.

18.§
Adatfeldolgozói tevékenység

145. 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.

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

147. 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.

148. 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.

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

150. 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.

19.§
Oktatás, tájékoztatás

151. Az Adatkezelő foglalkoztatotti állományába újonnan került olyan személyeket, akik munkakörüknél 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.

152. Az adatvédelmi tisztviselő az Adatkezelő személyes adatok kezelését végző személyi állományát a bekövetkezett adatvédelmi tárgyú jogszabály- és normaváltozásokról 15 napon belül köteles tájékoztatni, - különösen a jelentősebb adatvédelmi tárgyú normaváltozások vagy az ellenőrzés során feltárt visszatérő, vagy egyébként súlyos hiányosságok esetén - indokolt esetben az érintett állomány kötelező adatvédelmi oktatását elvégezni.

153. Az adatvédelmi tisztviselő az Adatkezelőnél az információszabadsággal összefüggő feladatok ellátásáért felelős személyi állomány közérdekű adatok nyilvánosságával összefüggő jogszabály- és normaváltozásokról történő tájékoztatásáért – különösen a jelentősebb normaváltozások vagy az ellenőrzés során feltárt visszatérő, vagy egyébként súlyos hiányosságok esetén – indokolt esetben az érintett állomány kötelező, információszabadság tárgyú oktatásának elvégezéséért.

20.§
Felülvizsgálat

154. Az Adatkezelő szervezeti egységei kötelesek a nyilvántartásba vett adatkezeléseiket félévente 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 el kell végezni. A felülvizsgálat körülményeit és eredményét írásban kell dokumentálni, az iratot tíz évig meg kell őrizni.

155. 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.

156. Ezen felülvizsgálat körülményeit és eredményét az Adatkezelő dokumentálja, e dokumentációt a felülvizsgálat elvégzését követő tíz évig megőrzi.

157. A Szabályzat mellékletei az adatkezelések olyan részeit rögzítik, amelyek azonnali módosítást igényelhetnek, ezért a mellékletek módosíthatók új főigazgatói utasítás nélkül amennyiben ezen módosítások érdemben nem hatnak ki a Szabályzatban foglalt főbb rendelkezésekre.

21.§
Panasztételi lehetőség

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

Nemzeti Adatvédelmi és Információszabadság Hatóság
1125 Budapest, Szilágyi Erzsébet fasor 22/C.
Levelezési cím: 1530 Budapest, Postafiók: 5.
Telefon: +36 -1-391-1400

Fax: +36-1-391-1410
E-mail: ugyfelszolgalat@naih.hu

22.§
Záró rendelkezés

A jelen szabályzat 2021. január 1. napján lép hatályba. A hatályba lépés napjával egyidejűleg hatályát veszti a Nemzeti Örökség Intézete Főigazgatójának 26/2019. (VIII.26.) főigazgatói utasítással kiadott Adatkezelési Szabályzata.

Az éves felülvizsgálat kezdeményezése és koordinálása a Jogi- és Humánpolitikai Igazgatóság feladata.

Budapest, 2020. december 23.

Nemzeti Örökség Intézete * 1. *

.....
Radnainé dr. Fogarasi Katalin
Főigazgató