



ORSZÁGOS VÍZÜGYI
FŐIGAZGATÓSÁG

Hatályos:
2025. 07. 22.

AZ ORSZÁGOS VÍZÜGYI FŐIGAZGATÓSÁG FŐIGAZGATÓJÁNAK

18/2025. (OVF) számú
UTASÍTÁSA

**Hatályon kívül
helyezve:**
30/2023. (OVF)
számú főigazgatói
utasítás, valamint
annak mellékletei

Mellékletek:
11 db

**Aktualizálás
gyakorisága,
rendje:**

Jelen utasítás
felülvizsgálatát
kétévente június
30. napjáig, vagy
jogszabályváltozást
követő 30 napon
belül kell elvégezni

**Aktualizálásért
felelős:**
Adatvédelmi
tisztviselő

AZ ORSZÁGOS VÍZÜGYI FŐIGAZGATÓSÁG ÉS A VÍZÜGYI IGAZGATÓSÁGOK ADATVÉDELMI ÉS ADATBIZTONSÁGI SZABÁLYZATA

Az Országos Vízügyi Főigazgatóság Szervezeti és Működési Szabályzatában foglalt felhatalmazás alapján, valamint a vízügyi igazgatási és a vízügyi, valamint a vízvédelmi hatósági feladatokat ellátó szervek kijelöléséről szóló 223/2014. (IX. 4.) Korm. rendelet 3/A. §-ban foglalt középírányítói feladatkörében eljárva – összhangban 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 Európai Parlament és a Tanács 2016. április 27-i (EU) 2016/679 számú rendeletének (a továbbiakban: GDPR) 24. cikk (2) bekezdésében, valamint az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvényben (a továbbiakban: Infotv.) foglalt rendelkezésekkel – az Országos Vízügyi Főigazgatóság és a vízügyi igazgatóságok (a továbbiakban: Adatkezelő) adatvédelmi és adatbiztonsági szabályzatát – az adatvédelmi tisztviselők bevonásával – az alábbi utasításban (a továbbiakban: Utasítás) foglaltak szerint adom ki:

I. FEJEZET BEVEZETŐ RENDELKEZÉSEK

1. Az Utasítás hatálya

- § Az Utasítás szervei hatálya az Adatkezelő szervezeti egységeire; személyi hatálya az Adatkezelő közalkalmazottaira, munkavállalóira és közfoglalkoztatottjaira, valamint az Adatkezelővel egyéb foglalkoztatási jogviszonyban álló személyekre (a továbbiakban: foglalkoztatottak) terjed ki.
- § Az Utasítás tárgyi hatálya az Adatkezelő kezelésében lévő személyes adatokra terjed ki, azaz minden olyan adatkezelésre, amely természetes személy – manuális módon és elektronikusan kezelt – adataira vonatkozik.

2. Az Utasításban foglaltak alkalmazási köre

- § (1) Az Utasításban foglaltakat kell alkalmazni az adatkezelési műveletekre az adatok megjelenési formájától függetlenül, az adatkezelés teljes folyamatára kiterjedően – az adatok megszerzésétől vagy az Adatkezelőnél történő keletkezésétől azok törléséig, illetve megsemmisítéséig –, függetlenül attól, hogy az adatok valamely nyilvántartási rendszer vagy valamely ügyben keletkezett irat részét képezik-e.

(2) Az Adatkezelő szerv adatkezelési tevékenységében állandó vagy eseti jelleggel résztvevő vagy abban közreműködő, az Adatkezelő szerv érdekkörében adatfeldolgozóként vagy közös adatkezelőként eljáró természetes vagy jogi személyekkel, jogi személyiséggel nem rendelkező szervezetekkel kötendő szerződésekben, megállapodásokban érvényesíteni kell jelen Utasításban meghatározott követelményeket a személyes adatok kezelésére vonatkozóan.

(3) A közérdekű és közérdekből nyilvános adatokra irányuló megkeresések esetében jelen Utasítást kell alkalmazni a megkeresésekben szereplő személyes adatok kezelése során.

(4) A nemzeti minősített adatok kezelésére vonatkozó jogszabály eltérő rendelkezésének hiányában jelen Utasítást kell alkalmazni a minősített adathordozón szerepeltetett személyes adatok kezelése során.

3. Értelmező rendelkezések

4. § Jelen Utasítás alkalmazásában

1. „Érintett”: bármely információ alapján azonosított vagy azonosítható természetes személy;
2. „Személyes adat”: az érintettre vonatkozó bármely információ;
3. „Adatkezelés”: az alkalmazott eljárástól függetlenül a személyes adaton végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtés, felvétel, 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;
4. „Adatkezelés korlátozása”: a tárolt személyes adat zárolása megjelöléssel további kezelés korlátozása céljából;
5. „Adatkezelő”: a Főigazgatóság esetében a Főigazgató és a vízügyi igazgatóság esetében az igazgató, aki az adat kezelésének célját és eszközeit meghatározza, az adatkezelésre vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja;
6. „Adatfeldolgozó”: az a természetes vagy jogi személy, jogi személyiséggel nem rendelkező szervezet, aki-, vagy amely az Adatkezelő megbízásából nevében, vagy rendelkezése szerint személyes adatokat kezel;
7. „Címzett”: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, akivel vagy amellyel a személyes adatot az Adatkezelő hozzáférhetővé teszi, függetlenül attól, hogy harmadik személy-e;
8. „Harmadik személy”: olyan természetes vagy jogi személy, jogi személyiséggel nem rendelkező szervezet, aki vagy 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 irányuló műveleteket végeznek;
9. „Az érintett hozzájárulása”: az érintett akaratának önkéntes, határozott és megfelelő tájékoztatáson alapuló egyértelmű kinyilvánítása, amellyel a rá vonatkozó személyes adatok kezeléséhez beleegyezését adja;
10. „Adatvédelmi incidens”: az adatbiztonság olyan sérülése, amely a kezelt személyes adatok véletlen vagy jogellenes megsemmisülését, elvesztését, módosulását, jogosulatlan továbbítását vagy nyilvánosságra hozatalát, vagy az azokhoz való jogosulatlan hozzáférést eredményezi;
11. „Felügyeleti hatóság”: a Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: NAIH);
12. „Adathordozó”: minden olyan anyagi eszköz, közeg, amely alkalmas adatok tárolására, megőrzésére. Fajtái: papíralapú, mágneses elven működő, optikai elven működő, magnetooptikai elven működő, elektronikus.
13. Kockázatbecslés: az Adatkezelő által a tervezett adatkezelési tevékenységet megelőzően végzett felmérés arra vonatkozóan, hogy a tervezett adatkezelés – célja, érintettek köre, alkalmazott technológiák – várhatóan milyen hatásokat fog gyakorolni az érintetteket megillető alapvető jogok érvényesülésére;

14. „Adatvédelmi hatásvizsgálat”: az Adatkezelő által készített írásbeli elemzés, abban az esetben, ha a kockázatbecslés során megállapítást nyer, hogy a tervezett adatkezelés magas kockázatú adatkezelés, azaz ha a tervezett adatkezelés valószínűsíthetően az érintetteket megillető, valamely alapvető jog érvényesülését lényegesen befolyásolja. Az egymáshoz hasonló típusú adatkezelési műveletek egyetlen hatásvizsgálat keretei között is értékelhetőek, amennyiben egymáshoz hasonló magas kockázatokat jelentenek;

15. „Adatkezelői nyilvántartás” az Adatkezelő személyes adatokra vonatkozó adatkezeléseiről, az adatvédelmi incidensekről és az érintett hozzáférési jogával kapcsolatos intézkedésekről vezetett nyilvántartása.

16. Magas kockázatú adatkezelés: olyan adatkezelés, amelyről az adatvédelmi hatásvizsgálat során megállapítást nyer, hogy az valószínűsíthetően lényegesen befolyásolni fogja az érintetteket megillető, valamely alapvető jog érvényesülését.

4. Elvek

5. § A személyes adatok kezelése során az Adatkezelő a GDPR 5. cikke szerinti elvek érvényre juttatásával köteles eljárni.

6. § A személyes adatok kezelésére vonatkozó elvek:

- a) jogszerűség, tisztességes eljárás és átláthatóság,
- b) célhoz kötöttség,
- c) adattakarékosság,
- d) pontosság,
- e) korlátozott tárolhatóság,
- f) integritás és bizalmas jelleg.

7. § Az Adatkezelő felel a 6. §-ban rögzített elveknek való megfelelésért, valamint a megfelelés igazolásáért (elszámoltathatóság elve).

8. § A 6. §-ban meghatározott kötelezettség kiterjed az Adatkezelő megbízásából adatfeldolgozó tevékenységet végző természetes vagy jogi személyekre, valamint jogi személyiséggel nem rendelkező személyekre is, mely kötelezettséget az Adatkezelő az adatfeldolgozóval kötött írásbeli szerződés útján érvényesít.

5. Az adatkezelés jogalapja

9. § Személyes adat – jogszabályi felhatalmazás hiányában – akkor kezelhető, ha

- a) az érintett hozzájárult személyes adatainak egy vagy több konkrét célból történő kezeléséhez,
- b) az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél, vagy az adatkezelés a szerződés megkötését megelőzően az érintett kérésére történő lépésekhez szükséges,
- c) az adatkezelés adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges,
- d) az adatkezelés az Érintett vagy más természetes személy létfontosságú érdekei védelme miatt szükséges,
- e) az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges,
- f) az adatkezelés az Adatkezelő vagy egy harmadik fél jogos érdekének érvényesítéséhez szükséges a GDPR 6. cikk f) pontjában meghatározott kivételekkel.

II. FEJEZET RÉSZLETES RENDELKEZÉSEK

6. Az adatkezelő feladatai

10. § Az adatkezelő megteszi az adatkezelés jogszerűségének biztosítása érdekében szükséges műszaki és szervezési intézkedéseket, továbbá felel

- a) az adatvédelmi és adatbiztonsági rendszer kialakításáért, irányításáért és rendeltetésszerű működtetéséért,
- b) az adatvédelmi feladatok ellátására alkalmas adatvédelmi tisztviselő kijelöléséért, nevének és elérhetőségeinek a NAIH részére történő bejelentéséért, valamint ezen adatoknak az Adatkezelő szerv honlapján történő közzétételéért,
- c) az adatvédelmi tisztviselő feladatainak végrehajtásához, a személyes adatokhoz és az adatkezelési műveletekhez való hozzáféréshez, valamint az adatvédelmi tisztviselő szakértői szintű ismereteinek fenntartásához szükséges feltételek és források biztosításáért valamint a NAIH által szervezett adatvédelmi tisztviselők konferencián való részvételéért,
- d) a belső adatvédelmi és adatbiztonsági szabályzat megalkotásáért, felülvizsgálataért az adatvédelmi tisztviselő bevonásával,
- e) a személyes adatok védelméhez és az információszabadsággal kapcsolatos követelmények érvényesüléséhez szükséges személyi, tárgyi és technikai feltételek biztosítását célzó, hatáskörébe tartozó intézkedések meghozataláért. Gondoskodik a személyes adatok körében a jogosulatlan hozzáférés, közlés, megváltoztatás vagy törlés megelőzéséről, a technikai védelemről, továbbá arról, hogy a személyes adatok védelmének biztosítása érdekében az Érintett az Adatkezelő által kezelt adataihoz – ha törvény kivételt nem tesz – hozzáférhessen, illetve gyakorolhassa a helyesbítéshez vagy törléshez való jogát,
- f) személyesen az általa vezetett szerv, illetve az irányítása alá tartozó szervezeti egységek tevékenységéért, azok törvényes és szakszerű működéséért, ezen belül az irányítása alatt álló állomány adatkezelésre vonatkozó tevékenységéért, az adatvédelmi előírások, valamint az iratkezelési és a nemzeti minősített adatra vonatkozó szabályok betartásáért,
- g) a rendszeres adatvédelmi ellenőrzésért, az ellenőrzés során esetlegesen feltárt hiányosságok vagy (jog)szabálysértő körülmények megszüntetéséért, a személyi felelősség megállapításához szükséges eljárás kezdeményezéséért, ennek érdekében a hatáskörébe tartozó eljárások lefolytatásáért,
- h) az érintett jogainak gyakorlásához, valamint tájékoztatásához szükséges feltételek biztosításáért,
- i) az adatvédelmi hatásvizsgálatok lefolytatásáért és rendszeres felülvizsgálataért, valamint az ahhoz szükséges feltételek biztosításáért,
- j) az adatvédelmi tevékenységgel kapcsolatos közzétételi kötelezettség teljesítéséért,
- k) a szervezeti egységek vezetője útján az adatkezelésekről történő nyilvántartás vezetéséért és annak rendszeres ellenőrzéséért,
- l) az adatvédelmi oktatásért és rendszeres továbbképzésért,
- m) az adatvédelmi incidensek megelőzéséért, kezeléséért, bekövetkezésekor gyors és hatékony reagálásról történő intézkedésért,
- n) az adatvédelmi incidens bekövetkezésekor szükség esetén az érintettek és a NAIH tájékoztatásáért.

7. Az adatvédelmi tisztviselő

11. § (1) Az adatvédelmi tisztviselő teljes szakmai függetlenséget élvez, feladatai ellátásával kapcsolatban utasításokat senkitől nem fogadhat el. Az Adatkezelő az adatvédelmi tisztviselőt feladatai jogszerű ellátásával összefüggésben hátrányos jogkövetkezménnyel – így különösen jogviszonyának megszüntetésével – nem sújthatja. Az adatvédelmi tisztviselő a Főigazgatóságon

közvetlenül a Főigazgatónak, a vízügyi igazgatóságon közvetlenül az Igazgatónak tartozik felelősséggel.

(2) Az Adatkezelő szerv vezetője az adatvédelmi tisztviselőt írásban jelöli ki. Adatvédelmi tisztviselőnek csak olyan személy jelölhető ki, aki a személyes adatok védelmére vonatkozó hazai és uniós jogi előírások és jogalkalmazási gyakorlat megfelelő szintű ismeretével rendelkezik és alkalmas az Infotv. 25/M. § (1) bekezdésében meghatározott feladatok ellátására. Adatvédelmi tisztviselőnek nem lehet olyan személyt kijelölni, aki az Adatkezelő szervnél adatkezeléssel kapcsolatos döntések meghozatalára jogosult személynek a Polgári Törvénykönyvről szóló 2013. évi V. törvény 8:1. § (1) bekezdés 2. pontja szerinti hozzátartozója. Az adatvédelmi tisztviselő az Adatkezelő szervnél más feladatokat is elláthat, azonban az Adatkezelő szerv köteles biztosítani, hogy ezekből a más feladatokból adódóan ne keletkezzen összeférhetetlenség, és az egyéb munkaköri feladatok ellátása nem veszélyeztetheti az adatvédelmi tisztviselői feladatok ellátását.

(3) Az adatvédelmi tisztviselő nevééről és elérhetőségéről az adatkezelő szervnél foglalkoztatottakat tájékoztatni kell, valamint a NAIH nyilvántartásába, a NAIH honlapján – www.naih.hu – található Adatvédelmi Tisztviselő Bejelentő Rendszer alkalmazásával be kell jelenteni. A bejelentés NAIH általi elfogadást követően az adatvédelmi tisztviselő adatait – név, postai levelezési cím, elektronikus levelezési cím, telefonszám – az Adatkezelő szerv honlapján fel kell tüntetni.

(4) Az adatvédelmi tisztviselő feladatainak ellátása céljából, az ahhoz szükséges mértékben a minősítéssel védett iratokba betekinthez.

(5) Az adatvédelmi tisztviselő a számára meghatározott feladatai kapcsán eljárva hozzáfér a feladatai végrehajtásához szükséges elektronikus rendszerekhez, iratokhoz, egyéb adathordozókhoz.

(6) Az Adatkezelőnél foglalkoztatottak a személyes adataik kezeléséhez és jogaik gyakorlásához kapcsolódó valamennyi kérdésben a hivatali út betartása nélkül, közvetlenül és egyszerű módon (így különösen személyesen: szóban vagy telefonon keresztül, valamint elektronikus úton) fordulhatnak az adatvédelmi tisztviselőhöz.

(7) Az Adatkezelő szerv vezetője köteles gondoskodni arról, hogy az adatvédelemmel kapcsolatos feladatokba az adatvédelmi tisztviselő soron kívül bevonásra kerüljön.

(8) Az adatvédelmi tisztviselő feladatai különösen:

- a) naprakész tájékoztatás nyújtása az adatvédelmet érintő jogi előírásokról és azok érvényesítéséről tanács adása a foglalkoztatottak részére,
- b) az adatkezelés folyamatos figyelemmel kísérése és ellenőrzése, hogy a GDPR-nak, az Infotv.-nek, valamint jelen Utasításnak megfeleljen,
- c) érintettek joggyakorlásának elősegítése – ide értve az adatkezelés jogszerűségével szembeni panaszok kivizsgálását és szükség esetén a panasz kivizsgálásához szükséges intézkedések megtételét,
- d) az adatvédelmi hatásvizsgálat lefolytatásában való közreműködés,
- e) a NAIH-hal együttműködés – ideértve az előzetes konzultációt és az eljárásokban való részvételt, közreműködés az adatvédelmi incidens kivizsgálásában, és a vizsgálat eredménye alapján – a jogszabályi feltételek fennállása esetén - az Adatkezelő szerv vezetőjének jóváhagyásával az adatvédelmi incidens a NAIH részére történő bejelentése, valamint az adatvédelmi incidens nyilvántartás vezetése,
- f) a belső adatvédelmi és adatbiztonsági szabályzat elkészítése,
- g) közreműködés a NAIH részére az Infotv. 30. § (3) bekezdés második fordulata alapján teljesítendő éves jelentés minden év január 31. napjáig történő elkészítésében.

(9) Az adatvédelmi tisztviselő a GDPR rendeletben és az Infotv.-ben rögzítetteken túl a következő feladatokat látja el:

- a) az adatkezeléssel kapcsolatos előírások megszegésének észlelése esetén az adatvédelmi tisztviselő felhív a jogszerű állapot haladéktalan helyreállítására, és a hiányosságokat – amennyiben emiatt adatvédelmi érdek sérelmet szenvedne, úgy közvetlenül – jelzi az adatkezelő szerv vezetőjének, indokolt esetben kezdeményezi a felelőség megállapításához szükséges eljárás lefolytatását;

- b) közreműködik az adatvédelmi incidensek kivizsgálásában, és a vizsgálat eredménye alapján a jogszabályi feltételek fennállása esetén bejelenti azt a NAIH részére;
- c) részt vesz a NAIH által szervezett képzéseken;
- e) koordinálja a szervezethez érkező általános közérdekű adat megismerésre vonatkozó igények teljesítését;
- f) véleményezi az adatfeldolgozóval kötendő megállapodást és a teljesítés igazolás előtt ellenőrzi a végrehajtás szabályszerűségét.

12. § Az adatkezelőnél lévő valamennyi szervezeti egység köteles

- a) az adatvédelmi tisztviselő felhívására soron kívül, az általa megjelölt időpontig tájékoztatást, felvilágosítást adni, adatot szolgáltatni,
- b) az adatvédelmi incidens megalapozott gyanúja esetén az incidenst és a bekövetkezésének körülményeit haladéktalanul bejelenteni.

8. Az adatvédelmi hatásvizsgálat lefolytatása

13. § (1) Az adatkezeléssel érintett szervezeti egység a tervezett adatkezelés megkezdését megelőzően kockázatbecsléssel felméri, hogy a tervezett adatkezelés annak körülményeire, így különösen céljára, az érintettek körére, az adatkezelési műveletek során alkalmazott technológiára tekintettel várhatóan milyen hatásokat fog gyakorolni az érintetteket megillető alapvető jogok érvényesülésére.

(2) Az adatkezeléssel érintett szervezeti egység az újonnan tervezett adatkezelésnél abban az esetben végez írásban előzetes adatvédelmi hatásvizsgálatot, ha az adatkezelés valamely - különösen új technológiákat alkalmazó - típusa, figyelemmel annak jellegére, hatókörére, körülményeire és céljára valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve. Korábban is végzett adatkezelés esetében az adatvédelmi hatásvizsgálatot az adatkezelés kockázatának és lényeges körülményeinek - különösen az adatkezelés technológiájának - megváltoztatása esetén kell elvégezni.

(3) Az adatkezeléssel érintett szervezeti egység a GDPR 35. cikkében rögzített adatvédelmi hatásvizsgálat lefolytatását az adatvédelmi tisztviselő szakmai tanácsa alapján végzi.

(4) Az adatvédelmi hatásvizsgálat kiterjed a tervezett adatkezelési műveletek módszeres leírására és az adatkezelés céljainak ismertetésére, az adatkezelés céljaira figyelemmel az adatkezelési műveletek szükségességi és arányossági vizsgálatára, az érintett jogait és szabadságait érintő kockázatok vizsgálatára és a kockázatok kezelését célzó intézkedések bemutatására.

(5) Az adatvédelmi hatásvizsgálat mintáját jelen Utasítás 1. sz. melléklete tartalmazza.

(6) Az adatkezeléssel érintett szervezeti egység szükség szerint, de legalább az adatkezelési műveletek által jelentett kockázat változása esetén ellenőrzést folytat le annak értékelése céljából, hogy a személyes adatok kezelése az adatvédelmi hatásvizsgálatnak megfelelően történik-e.

(7) Ha a vizsgálat alapján megállapítást nyer, hogy a tervezett adatkezelés nem magas kockázatú, vagy a tervezett adatkezelés az adatvédelmi hatásvizsgálat lefolytatása alóli mentesítést tartalmazó valamely jogszabályban meghatározott kivételi körbe tartozik, akkor ennek tényét az Adatkezelő írásban rögzíti.

(8) Adatvédelmi hatásvizsgálat lefolytatására kerül sor az adatkezeléssel érintett szervezeti egység részéről, amennyiben a kockázatbecslés során az adatkezeléssel érintett szervezeti egység az adatkezeléssel várhatóan érintett személyek jogaira és szabadságaira nézve magas kockázatot állapít meg vagy jogszabályi rendelkezés alapján adatvédelmi hatásvizsgálattal kötelezően vizsgálandó adatkezelési tevékenységek esete áll fenn.

(9) A Főigazgatóság esetén a főigazgató vagy a vízügyi igazgatóságok esetén az igazgató a feladattal érintett szervezeti egység vezetője javaslatára elrendeli az adatvédelmi hatásvizsgálat lefolytatását vagy írásban rögzíti mellőzésének okait, és az adatvédelmi tisztviselő kapcsolódó álláspontját.

- (10) Az adatvédelmi hatásvizsgálat lefolytatásában az adatkezelés által érintettek vesznek részt. Az adatvédelmi hatásvizsgálat lefolytatásában az adatvédelmi tisztviselő közreműködik minden esetben.
- (11) Az adatvédelmi tisztviselő az adatvédelmi hatásvizsgálatokról nyilvántartást vezet jelen Utasítás 2. sz. melléklete szerint.

9. Az előzetes konzultáció kezdeményezése

14. § (1) Ha az adatvédelmi hatásvizsgálat során megállapítást nyer, hogy az adatkezelés az adatkezeléssel érintett szervezeti egység által a kockázat mérséklése céljából tett intézkedések hiányában valószínűsíthetően magas kockázattal jár, a személyes adatok kezelését megelőzően az Adatkezelő konzultációt kezdeményez a NAIH-nál.

(2) Az Adatkezelő a konzultáció során a NAIH-ot tájékoztatja:

- a) az Adatkezelő (közös Adatkezelők, adatfeldolgozók) feladatköreiről,
- b) a tervezett adatkezelés céljairól és módjairól,
- c) az érintettek jogainak és szabadságainak védelmében hozott intézkedésekről és garanciákról,
- d) az adatvédelmi tisztviselő elérhetőségeiről,
- e) az adatvédelmi hatásvizsgálatról és
- f) a NAIH által kért minden egyéb információról.

(3) Az Adatkezelő a konzultációt követően a NAIH által meghatározott javaslatok figyelembevételével jár el.

10. Az adatvédelmi incidens kezelésének eljárásrendje

10.1. Az adatvédelmi incidensek észlelése

15. § (1) A foglalkoztatottak kötelesek az adatvédelmi incidens gyanúját a szervezeti egység vezetője útján az Adatkezelő szerv vezetőjének haladéktalanul jelenteni. A szervezeti egység vezetője tudomására jutását követően azonnal köteles az adatvédelmi tisztviselőt és szükség esetén az IT biztonsági felelőst, a Főigazgatóság esetében az Informatikai és Téradat Főosztály vezetőjét, a vízügyi igazgatóság esetében az Informatikai és Téradat Osztály vezetőjét az adatvédelmi incidens gyanújában kivizsgálási eljárásának lefolytatásába bevonni.

(2) Amennyiben az (1) bekezdésben szereplő bejelentés külső személytől vagy szervtől érkezik, akkor a bejelentést a feladat- és hatáskörrel rendelkező szervezeti egység vezetőjéhez soron kívül kell továbbítani. A szervezeti egység vezetője köteles az adatvédelmi tisztviselőt és szükség esetén az IT biztonsági felelőst, a Főigazgatóság esetében az Informatikai és Téradat Főosztály vezetőjét, a vízügyi igazgatóság esetében az Informatikai és Téradat Osztály vezetőjét az eljárás lefolytatásába bevonni.

(3) Az IT biztonsági felelős megvizsgálja, hogy

- a) IT biztonsági incidens bekövetkezett-e,
- b) mely szervezeti egységek vezetőit kell bevonni az intézkedések megtételére.

(4) Az IT biztonsági felelős az IT biztonsági incidens gyanúja felmerülése esetén a döntés-előkészítő iratot az érintett szervezeti egység vezetője – részére továbbítja, az első számú vezető valamint az adatvédelmi tisztviselő egyidejű tájékoztatásával.

(5) Ha nem állapítható meg IT biztonsági incidens, úgy a többi belső normatív utasításban szereplő eljárásrend alapján szükséges eljárni.

10.2. A bejelentés megvizsgálása és az adatvédelmi incidens kezelése

16. § (1) A 15. § szerinti bejelentés esetén a Főigazgatóság esetében a főigazgató, a vízügyi igazgatóság esetében az igazgató – az adatvédelmi tisztviselő és szükség esetén a Főigazgatóság esetében az Informatikai és Téradat Főosztály vezetője, a vízügyi igazgatóság esetében az Informatikai és Téradat Osztály vezetője és az IT biztonsági felelős bevonásával – a bejelentés megvizsgálásáról haladéktalanul intézkedik.

(2) Ha a vizsgálat során megállapítást nyer, hogy az érintettek jogaival és szabadságaival kapcsolatban magas kockázat áll fenn, akkor az Adatkezelő az adatvédelmi tisztviselő közreműködésével az adatvédelmi incidenst a NAIH részére indokolatlan késedelem nélkül, legkésőbb azonban az adatvédelmi incidens tudomásra jutásától számított 72 órán belül bejelenti a NAIH honlapján – www.naih.hu – található Adatvédelmi Incidensbejelentő Rendszeren keresztül. Az Adatkezelő az adatvédelmi tisztviselő közreműködésével a bejelentéssel egyidejűleg kitölti a jelen Utasítás 3. sz. melléklete szerinti formanyomtatványt.

(3) Az Adatkezelő az adatvédelmi incidens bejelentését mellőzi, ha az valószínűsíthetően nem jár magas kockázattal a természetes személyek jogaira és szabadságaira nézve.

(4) Ha a bejelentés nem történik meg 72 órán belül, a NAIH-ot a késedelem igazolására szolgáló indokairól is tájékoztatni kell.

(5) 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 jelen Utasítás 4. sz. melléklete szerinti tartalommal, a GDPR 34. cikke alapján.

(6) Az adatvédelmi tisztviselő az adatvédelmi incidensekről jelen Utasítás 5. sz. melléklete szerinti nyilvántartást vezet.

11. Az érintett jogai, valamint az érintett jogainak érvényesítésével összefüggő feladatok

17. § (1) Az érintett jogait a GDPR III. fejezetének rendelkezései rögzítik. Az érintettnek joga van

a az átlátható tájékoztatáshoz,

b) a tájékoztatáshoz és a személyes adatokhoz való hozzáféréshez,

c) a személyes adatok helyesbítéséhez, törléséhez (elfeledtetéshez való jog),

d) az adatkezelés korlátozásához,

e) a címzettekről a c) és d) pontok vonatkozásában az értesítéshez,

f) az adathordozhatósághoz,

g) az adatai meghatározott körben történő kezelése elleni tiltakozáshoz ideértve a profilalkotást is,

h) az adatvédelmi incidensről való tájékoztatáshoz.

(2) Az érintett jogosult az adatvédelmi tisztviselőhöz, a NAIH-hoz (panasztétel joga), valamint ha a Hatóság a jogszabályban megadott határidőn belül nem ad tájékoztatást, a bírósághoz fordulni (jogorvoslati jogosultság).

18. § (1) Az Adatkezelő köteles az érintettek joggyakorlást biztosítani, ennek keretében a kérelmező megfelelő azonosítását követően a kérelem tartalmát kell hitelesítenie. Az egyértelmű azonosításhoz szükségesek a kérelmező nevének túl az Adatkezelő által kezelt személyes adatok.

(2) Az Adatkezelő az érintettet könnyen hozzáférhető formában – írásban, elektronikus úton vagy szóban – és közérthető tartalommal tájékoztatja a kérelemben foglaltaknak megfelelően. Az Adatkezelő indokolatlan késedelem nélkül, de legfeljebb a kérelem beérkezésétől számított egy hónapon belül tájékoztatja az érintettet. A GDPR 12. cikk alapján a teljesítési határidő – az érintett egyidejű tájékoztatásával, valamint az indokok megjelölésével – két hónappal meghosszabbítható.

(3) Az Adatkezelő az első másolatot díjmentesen biztosítja az érintett részére. Amennyiben ugyanazon kérelmező, ugyanolyan tartalmú kérelmet terjeszt elő, úgy az Adatkezelő a további másolatért az Országos Vízügyi Főigazgatóságnak és a vízügyi igazgatóságoknak a közérdekű adatok megismerésére és a szolgáltatási szerződés megkötésére vonatkozó eljárásrendjéről szóló főigazgatói utasítás szerinti díjat állapíthat meg.

(4) Az Adatkezelő az érintettek joggyakorlásáról jelen Utasítás 6. sz. melléklete szerinti nyilvántartást vezet.

12. Az adatkezelési tevékenységek nyilvántartása

19. § (1) Az Adatkezelő nyilvántartást vezet a feladat- és hatásköre alapján végzett adatkezelési tevékenységekről.

(2) Az Adatkezelő köteles a NAIH-hal együttműködni és a nyilvántartásokat kérésre hozzáférhetővé tenni az érintett adatkezelési műveletek ellenőrzése érdekében.

(3) Jelen Utasításban foglaltaknak megfelelően úgy kell kialakítani és működtetni az adatvédelmi nyilvántartás feltételeit, hogy azok biztosítsák különösen a jogosulatlan hozzáférés, megsemmisülés, megváltoztatás megakadályozását.

(4) Az adatkezelési tevékenységek nyilvántartása tartalmazza különösen

- a) az Adatkezelő nevét és elérhetőségét, képviselője nevét és elérhetőségét, az adatvédelmi tisztviselő nevét és elérhetőségét, szükség esetén a közös adatkezelő, valamint az adatfeldolgozó nevét és elérhetőségét, képviselője nevét és elérhetőségét,
- b) az adatkezelés célját,
- c) az érintettek körét,
- d) a személyes adatok kategóriáját,
- e) a címzettek kategóriáját,
- f) a személyes adatok továbbítására vonatkozó információt,
- g) a személyes adatok törlésére előírányzott határidőt,
- h) a technikai és szervezési intézkedések általános leírását.

(5) A GDPR 30. cikk (1) bekezdése szerinti adatkezelési nyilvántartás irányadó mintáját jelen Utasítás 7. számú melléklete tartalmazza.

(6) Az (5) bekezdés szerint készült nyilvántartást az önálló szervezeti egységek vezetői az adatvédelmi tisztviselő közreműködésével készítik el, és a közös meghajtón kötelesek változás esetén azonnal a legfrissebb nyilvántartást menteni, a korábbi nyilvántartások egyidejű megtartásával.

13. Adattovábbítás, adattovábbítási nyilvántartás

20. § (1) Az Adatkezelő az adattovábbítást megelőzően köteles ellenőrizni

- a) az adattovábbítás feltételeinek és a célhoz kötöttség meglétét (jogszerű adattovábbítás),
- b) azt, hogy az adatkérő rendelkezik-e az adatkezeléshez szükséges jogalappal, vagy
- c) az érintett hozzájárult-e a személyes adatainak továbbításához.

(2) Az adatigénylés az adatvédelmi tisztviselő véleményének kikérését követően abban az esetben teljesíthető, ha a kérelem tartalmazza

- a) az adatigénylés célját, jogalapját (jogszerű adattovábbítás),
- b) a személyes adatok pontos meghatározását,
- c) az érintett azonosításához szükséges adatokat.

(3) Az adattovábbítás formája lehet

- a) kérelem alapján egyedi adatszolgáltatásra vonatkozóan elektronikus vagy papír alapú,
- b) törvény vagy erre vonatkozó megállapodás alapján közvetlen hozzáférés.

21. § (1) Az adattovábbítási nyilvántartás tartalmazza

- a) az Adatkezelő nevét és elérhetőségét, képviselője nevét és elérhetőségét, az adatvédelmi tisztviselő nevét és elérhetőségét, szükség esetén a közös adatkezelő, valamint az adatfeldolgozó nevét és elérhetőségét, képviselője nevét és elérhetőségét,
- b) az adattovábbítás dátumát,
- c) az érintett beazonosításához szükséges adatokat,
- d) az adattovábbítás célját,
- e) az adattovábbítás jogalapját,
- f) az átadott adatok körét,
- g) az adattovábbítás címzettjét.

- (2) A nyilvántartást elektronikus úton és papír alapon is lehet vezetni.
(3) Az adattovábbítási nyilvántartást jelen Utasítás 8. sz. melléklete tartalmazza.

14. Adattörlés, adattörlési nyilvántartás, megsemmisítési jegyzőkönyv

22. § (1) Az Adatkezelő indokolatlan késedelem nélkül köteles törölni az érintett személyes adatait, amennyiben az alábbi indokok valamelyike fennáll
- a) a személyes adatokra már nincs szükség (az adatkezelés célja megszűnt),
 - b) az érintett a hozzájárulását visszavonta és az adatkezelésnek nincs más jogalapja,
 - c) az érintett tiltakozása esetén,
 - d) az Adatkezelő a személyes adatokat jogellenesen kezelte,
 - e) a személyes adatokat az Adatkezelőre vonatkozó jogszabályi kötelezettség teljesítéséhez törölni kell.
- (2) Az adattörlési nyilvántartás tartalmazza
- a) a kérelem időpontját,
 - b) a kérelmező nevét, elérhetőségét,
 - c) a kérelem tartalmát – ideértve az adattörlés célját, a személyes adatok körét,
 - d) a megtett intézkedéseket,
 - e) a törlés indokát,
 - f) az adatok törlésének időpontját,
 - g) az adattörlést végző foglalkoztatott nevét, beosztását, szervezeti egységét.
- (3) A személyes adatok megsemmisítési jegyzőkönyv felvételével semmisíthetők meg.
(4) Az adattörlési nyilvántartást jelen Utasítás 9. sz. melléklete, a megsemmisítési jegyzőkönyvet jelen Utasítás 10. sz. melléklete rögzíti.

15. Adatfeldolgozó igénybevétele, adatfeldolgozói nyilvántartás

23. § (1) Az Adatkezelő az adatok feldolgozásával kapcsolatos műveletek elvégzésére Adatfeldolgozót vehet igénybe. Az Adatfeldolgozónak a személyes adatok feldolgozásával kapcsolatos jogait és kötelezettségeit a GDPR, valamint a vonatkozó jogszabályok keretei között az Adatkezelő határozza meg szerződésben. Az adatfeldolgozásra vonatkozó megbízási szerződést írásba kell foglalni.
- (2) Az adatfeldolgozói nyilvántartás tartalmazza
- a) az Adatfeldolgozó nevét, elérhetőségeit, képviselője nevét, elérhetőségeit, adatvédelmi tisztviselője nevét, elérhetőségeit,
 - b) az Adatkezelő nevét, elérhetőségeit, képviselője nevét, elérhetőségeit, adatvédelmi tisztviselője nevét, elérhetőségeit,
 - c) az Adatkezelő nevében végzett adatkezelési tevékenységek kategóriát,
 - d) a személyes adatok körét,
 - e) az érintettek körét,
 - f) szükség esetén az adattovábbítás tényét,
 - g) a technikai és szervezési intézkedések általános leírását,
 - h) a szerződés iktatószámát.
- (3) Az adatfeldolgozói nyilvántartás mintáját jelen Utasítás 11. sz. melléklete rögzíti.

16. Adatbiztonsági (technikai és szervezési) intézkedések

24. § (1) Az Adatkezelő a személyes adatok biztonsága érdekében megteszi azokat a technikai és szervezési intézkedéseket és kialakítja azokat az eljárási szabályokat, amelyek különösen a GDPR-ban foglalt rendelkezések érvényre juttatásához szükségesek.
- (2) Az Adatkezelő az adatokat megfelelő intézkedésekkel védi a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, a véletlen

megsemmisülés és sérülés, továbbá az alkalmazott technika megváltoztatásából fakadó hozzáférhetetlenné válás ellen.

(3) Az Adatkezelő a személyes adatokat bizalmas adatként minősíti és kezeli. Az Adatkezelőt titoktartási kötelezettség terheli a személyes adatok kezelésére vonatkozóan. A személyes adatokhoz való hozzáférést az Adatkezelő jogosultsági szintek megadásával korlátozza.

(4) Az Adatkezelő az informatikai rendszereket tűzfalal védi, és vírusvédelemmel látja el.

(5) Az Adatkezelő az elektronikus adatfeldolgozást, nyilvántartást számítógépes program útján végzi, amely megfelel az adatbiztonság követelményeinek. A program biztosítja, hogy az adatokhoz csak célhoz kötötten, ellenőrzött körülmények között csak azon személyek férjenek hozzá, akiknek a feladataik ellátása érdekében erre szükségük van.

(6) A személyes adatok automatizált feldolgozása során az Adatkezelő további intézkedésekkel biztosítja

a) a jogosulatlan adatbevitel megakadályozását,

b) az automatikus adatfeldolgozó rendszerek jogosulatlan személyek általi, adatátviteli berendezés segítségével történő használatának megakadályozását,

c) annak ellenőrizhetőségét és megállapíthatóságát, hogy a személyes adatokat adatátviteli berendezés alkalmazásával mely szerveknek továbbították vagy továbbíthatják,

d) annak ellenőrizhetőségét és megállapíthatóságát, hogy mely személyes adatokat, mikor és ki rögzítette az automatikus adatfeldolgozó rendszerekbe,

e) a telepített rendszerek üzemzavar esetén történő helyreállíthatóságát és

f) azt, hogy az automatizált feldolgozás során fellépő hibákról jelentés készüljön,

g) a személyes adat teljes életciklusa során, a személyes adatok bizalmasságát, sértetlenségét és rendelkezésre állását.

(7) Az Adatkezelő a személyes adatok védelme érdekében gondoskodik az elektronikus úton folytatott bejövő és kimenő kommunikáció ellenőrzéséről.

(8) Az Adatkezelő által kezelt személyes adatok interneten történő megosztása szigorúan tilos.

(9) A munkahelyen és a vízügyi ágazat eszközein a hatályos informatikai biztonsági szabályzat szerint kell eljárni.

(10) Külső forrásból kapott vagy letöltött, nem engedélyezett programok használata szigorúan tilos.

(11) A folyamatban levő munkavégzés, feldolgozás alatt levő iratokhoz csak az illetékes ügyintézők férhetnek hozzá, a személyzeti, a bér- és munkaügyi adatokat tartalmazó iratokat biztonságosan, zárható páncélszekrényben elzárva kell tartani.

(12) Az Adatkezelő biztosítja az adatok és az adathordozó eszközök, iratok megfelelő fizikai védelmét.

17. Oktatás, vizsgáztatás

25. § (1) A vízügyi igazgatási szervhez újonnan belépő foglalkoztatottak adatvédelmi oktatásban részesülnek.

(2) Az Adatkezelő a GDPR-ban és az Infotv.-ben meghatározott főbb szabályok ismertetése céljából adatvédelmi oktatást szervez a foglalkoztatottak részére.

(3) Az adatvédelmi oktatás módját, tematikáját, feltételeit, a vizsgáztatás rendjéte főigazgató és az igazgatók határozzák meg. A továbbképzés a BM RVTV portálon választható képzéssel is teljesíthető.

III. FEJEZET ZÁRÓ RENDELKEZÉSEK

26. § Jelen Utasítás a közzétételét követő munkanapon lép hatályba, amellyel egyidejűleg hatályát veszti a 30/2023. (OVF) számú főigazgatói utasítás, valamint mellékletei.

27. § Az Igazgatóságok jelen Utasítás hatályba lépését követő 30 napon belül kötelesek felülvizsgálni és szükség szerint módosítani az Igazgatóságukra vonatkozó részletszabályokat, amelyek nem lehetnek ellentétesek a vonatkozó jogszabályok és jelen Utasítás rendelkezéseivel.

28. § Jelen Utasítás felülvizsgálatáért és aktualizálásáért az adatvédelmi tisztviselő felel, a felülvizsgálatot két évente június 30. napjáig, vagy jogszabályváltozást követő 30 napon belül el kell végezni.

29. § Jelen Utasításban foglaltakat a Főigazgatóság és a vízügyi igazgatóságok valamennyi foglalkoztatottja köteles megismerni és betartani.

30. § Jelen Utasításban foglaltak betartásáért a Főigazgató és az Igazgatók, valamint valamennyi szervezeti egység vezetője az általa irányított szervezeti egység vonatkozásában felelősséggel tartozik.

31. § Jelen Utasítást és mellékleteit az Adatkezelő köteles közzétenni honlapján, megfelelő fejléc alkalmazásával, letölthető formátumban.

Budapest, 2025. július 21.



Láng István
főigazgató

Mellékletek:

1. sz. melléklet: Adatvédelmi hatásvizsgálat
2. sz. melléklet: Adatvédelmi hatásvizsgálat nyilvántartása
3. sz. melléklet: Adatvédelmi incidens bejelentése a Nemzeti Adatvédelmi és Információszabadság Hatósághoz
4. sz. melléklet: Az érintett tájékoztatása adatvédelmi incidensről
5. sz. melléklet: Adatvédelmi incidens nyilvántartás
6. sz. melléklet: Érintettek joggyakorlásának nyilvántartása
7. sz. melléklet: Adatkezelési tevékenységek nyilvántartása
8. sz. melléklet: Adattovábbítási nyilvántartás
9. sz. melléklet: Adattörlési nyilvántartás
10. sz. melléklet: Megsemmisítési jegyzőkönyv
11. sz. melléklet: Adatfeldolgozói nyilvántartás