Hatályos:
2023. 10. 16.

Hatályon kívül helyezve:
28/2021. (OVF) számú főigazgatói utasítás, valamint annak mellékletei

Aktualizálás gyakorisága, rendje:
jogszabályváltozást követő 30 napon belül, de legalább kétévente

Mellékletek:
11 db

Aktualizálásért felelős:
Főigazgatói Hivatal vezetője

AZ ORSZÁGOS VÍZÜGYI FŐIGAZGATÓSÁG FŐIGAZGATÓJÁNAK

30/2023. (OVF) számú

UTASÍTÁSA

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

Az Országos Vízügyi Főigazgatóság (a továbbiakban: Főigazgatóság) Szervezeti és Működési Szabályzatáról szóló 7/2019. számú OVF Főigazgatói Utasítás 26. (3) bekezdésének felhatalmazása alapján – 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 tisztviselő bevonásával – az alábbi utasításban (a továbbiakban: Utasítás) foglaltak szerint adom ki:

I. ÁLTALÁNOS RENDELKEZÉSEK

1. Az Utasítás hatálya

1.§ Az Utasítás szervi 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.
2. § 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

3. § (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

központi telefonszám: +36 1 225-4400 • cím: 1012 Budapest, Márvány utca 1/d • levélcím: 1253 Budapest, Pf. 56.
email-cím: ovf@ovf.hu • honlap: www.ovf.hu

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 adathordozóban szerepeltetett személyes adatok kezelése során.

3. Értelmező rendelkezések

4. § Jelen Utasítás alkalmazásában

1. „Érintett”: azonosított vagy azonosítható természetes személy;
2. „Személyes adat”: az érintettre vonatkozó bármely információ;
3. „Adatkezelés”: a személyes adaton végzett bármely művelet vagy a műveletek összessége, így különösen 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;
4. „Adatkezelés korlátozása”: a tárolt személyes adat megjelölése jövőbeli kezelése 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, közhatalmi szerv, jogi személyiséggel nem rendelkező szervezet, aki, vagy amely az Adatkezelő nevében személyes adatokat kezel;
7. „Címzett”: az a természetes vagy jogi személy, közhatalmi szerv, jogi személyiséggel nem rendelkező szervezet, akivel vagy amellyel a személyes adatot az Adatkezelő közli, függetlenül attól, hogy harmadik személy-e – ide nem értve a közhatalmi szervek által végzett egyedi vizsgálatot;
8. „Harmadik személy”: olyan természetes vagy jogi személy, közhatalmi szerv, 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 felhatalmazást kaptak;
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”: a biztonság 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: Hatóság);
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. „Adatvédelmi hatásvizsgálat”: egy olyan eljárás, amelynek során az Adatkezelő a tervezett adatkezelési műveletet vagy műveleteket áttekinti, megvizsgálja az adatkezelés érintettekre gyakorolt esetleges hatását, felméri azok kockázatait, a kockázatok kezelésének módját, és mindezt megfelelően dokumentálja. Ha az adatkezelés valamely típusa – különösen új technológiák alkalmazása –, figyelemmel annak jellegére, hatókörére, körülményére és céljaira,

valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, akkor az Adatkezelő az adatkezelést megelőzően hatásvizsgálatot végez arra vonatkozóan, hogy a tervezett adatkezelési műveletek a személyes adatok védelmét hogyan érintik. Az egymáshoz hasonló típusú adatkezelési műveletek egyetlen hatásvizsgálat keretei között is értékelhetőek, amennyiben egymáshoz hasonló magas kockázatokat jelentenek;

14. „Adatvédelmi nyilvántartás": az Adatkezelő személyes adatokra vonatkozó adatkezeléseiről, az érintettek joggyakorlásának elősegítése és az Adatkezelőre vonatkozó elszámoltathatóság elvének való megfelelés, valamint a jogszerű adatkezelés érdekében nyilvántartást vezet.

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).

5. Az adatkezelés jogalapja

8. § 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 vagy a szerződés létrejöttét megelőző lépésekhez szükséges, amelyben az Érintett szerződő fél,
c) az adatkezelés jogi kötelezettség teljesítéséhez szükséges,
d) az adatkezelés az Érintett vagy más természetes személy létfontosságú érdekei védelme miatt szükséges,
e) az adatkezelés közérdekű feladat végrehajtásához vagy közhatalmi jogosítvány gyakorlásához szükséges.
f) az adatkezelés az Adatkezelő vagy egy harmadik fél jogos érdekének érvényesítéséhez szükséges

II. RÉSZLETES RENDELKEZÉSEK

1. A főigazgató és az igazgató feladatai

9. § A főigazgató és az igazgató felel

a) az adatvédelmi és adatbiztonsági rendszer kialakításáért, irányításáért és rendeltetésszerű működtetéséért,

b) a belső adatvédelmi és adatbiztonsági szabályzat megalkotásáért az adatvédelmi tisztviselő bevonásával,

c) 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,
d) 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,
e) 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,
f) az érintett jogainak gyakorlásához, valamint tájékoztatásához szükséges feltételek biztosításáért,
g) az adatvédelmi hatásvizsgálatok lefolytatásáért és rendszeres felülvizsgálatáért, valamint az ahhoz szükséges feltételek biztosításáért,
h) az adatvédelmi feladatok ellátására alkalmas adatvédelmi tisztviselő kijelöléséért, nevének és elérhetőségeinek a Hatóság részére történő bejelentéséért, valamint ezen adatoknak az Adatkezelő szerv honlapján történő közzétételéért,
i) 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,
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 Hatóság tájékoztatásáért.

2. Az adatvédelmi tisztviselő

10. § (1) Az adatvédelmi tisztviselő teljes szakmai függetlenséget élvez, feladatai ellátásával kapcsolatban utasításokat senkitől nem fogad el. Az Adatkezelő az adatvédelmi tisztviselőt feladatai ellátásával összefüggésben nem bocsáthatja el és szankcióval nem sújthatja. Az adatvédelmi tisztviselő a Főigazgatóságon közvetlenül 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 személyi biztonsági feltételeknek megfelel. 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. § 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 nevéről és elérhetőségéről az adatkezelő szervnél foglalkoztatottakat tájékoztatni kell, valamint a Hatóság nyilvántartásába, a Hatóság honlapján – www.naih.hu – található Adatvédelmi Tisztviselő Bejelentő Rendszer alkalmazásával be kell jelenteni. A bejelentés Hatóság 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 számára feladatainak ellátása céljából, az ahhoz szükséges mértékben a minősítéssel védett iratokba betekinthet.

(5) Az Adatkezelő szerv vezetője biztosítja az adatvédelmi tisztviselő számára meghatározott feladata kapcsán eljárva a hozzáférést a feladatai végrehajtásához szükséges elektronikus rendszerekhez, iratokhoz, egyéb adathordozókhoz, valamint a szakmai ismeretei naprakészen tartásához szükséges feltételeket, jogosultságokat és erőforrásokat rendelkezésére bocsátja.
(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 tájékoztatást nyújt az adatvédelmet érintő jogi előírásokról és azok érvényesítéséről tanácsot ad a foglalkoztatottak részére,
b) folyamatosan figyelemmel kíséri és ellenőrzi a GDPR-nak, az Infotv.-nek, valamint jelen Utasításnak való megfelelést,
c) érintettek joggyakorlásának elősegítése – ide értve a panaszok kivizsgálását és szükség esetén a panasz orvoslásához szükséges intézkedések megtételét,
d) az adatvédelmi hatásvizsgálat lefolytatásában való közreműködés,
e) együttműködik a Hatósággal – ideértve az előzetes konzultációt és az eljárásokban való részvételt, közreműködik az adatvédelmi incidens kivizsgálásában, és a vizsgálat eredménye alapján – a jogszabályi feltételek fennállása esetén - az Adatkezelő szerv vezetőjének jóváhagyásával az adatvédelmi incidens Hatóság részére történő bejelentésért, valamint az adatvédelmi incidens nyilvántartás vezetéséért,
f) közreműködik a belső adatvédelmi és adatbiztonsági szabályzat megalkotásában.
g) az adatvédelmi tisztviselő közreműködik a Hatóság részére az Infotv. 30. § (3) bekezdés második fordulata alapján teljesítendő éves jelentés minden év január 31. napjáig történő elkészítésében.

3. Az adatvédelmi hatásvizsgálat lefolytatása

11. § (1) Az Adatkezelő abban az esetben végez adatvédelmi hatásvizsgálatot, ha az adatkezelés valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve.
(2) Az Adatkezelő a GDPR 35. cikkében rögzített adatvédelmi hatásvizsgálat lefolytatását az adatvédelmi tisztviselő szakmai tanácsa alapján végzi.
(3) 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.
(4) Az adatvédelmi hatásvizsgálat mintáját jelen Utasítás 1. sz. melléklete tartalmazza.
(5) Az Adatkezelő 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.
(6) Ha a vizsgálat alapján megállapítást nyer, hogy valószínűsíthetően magas kockázat azonosítására nem került sor, vagy az adatkezelés az adatvédelmi hatásvizsgálat lefolytatása alóli mentesítést tartalmazó valamely jogszabályban meghatározott kivételi körbe tartozik, akkor ennek tényét az Adatkezelő írásban rögzíti.
(7) Amennyiben az Adatkezelő az adatkezeléssel várhatóan érintett személyek jogaira és szabadságaira nézve magas kockázatot azonosít vagy jogszabályi rendelkezés lapján adatvédelmi hatásvizsgálattal kötelezően vizsgálandó adatkezelési tevékenységek esete áll fenn, adatvédelmi hatásvizsgálat lefolytatására kerül sor.

(8) 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.
(9) Az adatvédelmi hatásvizsgálat lefolytatásában az adatkezelés által érintettek vesznek részt. Az adatvédelmi hatásvizsgálat lefolytatásában az adatvédelmi tisztviselő közreműködik.
(10) Az adatvédelmi tisztviselő az adatvédelmi hatásvizsgálatokról nyilvántartást vezet jelen Utasítás 2. sz. melléklete szerint.

4. Az előzetes konzultáció kezdeményezése

12. § (1) Ha az adatvédelmi hatásvizsgálat során megállapítást nyer, hogy az adatkezelés az Adatkezelő által a kockázat mérséklése céljából tett intézkedések hiányában valószínűsíthetően magas kockázattal jár, a személyes adatok kezelését megelőzően az Adatkezelő konzultációt kezdeményez a Hatóságnál.
(2) Az Adatkezelő a konzultáció során a Hatóságot 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 Hatóság által kért minden egyéb információról.
(3) Az Adatkezelő a konzultációt követően a Hatóság tanácsainak figyelembevételével jár el.

5. Az adatvédelmi incidenskezelési eljárásrend

5.1. Az adatvédelmi incidensek észlelése

13. § (1) A foglalkoztatottak kötelesek az adatvédelmi incidens gyanúját a szervezeti egység vezetője útján az Adatkezelő szerv vezetőjének jelenteni. A szervezeti egység vezetője köteles az adatvédelmi tisztviselőt és szükség esetén az IT biztonsági felelőst, a Főigazgatóság esetében az Informatikai Főosztály vezetőjét, a vízügyi igazgatóság esetében az Informatikai Osztály vezetőjét az eljárás 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 Főosztály vezetőjét, a vízügyi igazgatóság esetében az Informatikai Osztály vezetőjét az eljárás lefolytatásába bevonni.
(3) Az IT biztonsági felelős megvizsgálja, hogy
a) IT biztonsági incidens bekövetkezette-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 – ennek hiányában a Főigazgatóság esetében a Főigazgatói Hivatal vezetője, a vízügyi igazgatóság esetében az igazgató – részére továbbítja, az adatvédelmi tisztviselő egyidejű tájékoztatásával.
(5) Ha nem állapítható meg IT biztonsági incidens, úgy a többi belső normatív utasításban szereplő eljárásrend alapján szükséges eljárni.

5.2. A bejelentés megvizsgálása és az adatvédelmi incidens kezelése

14. § (1) A 13. § 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 Főosztály vezetője, a vízügyi igazgatóság esetében az Informatikai 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 Hatóság részére indokolatlan késedelem nélkül, legkésőbb azonban az adatvédelmi incidens tudomásra jutásától számított 72 órán belül bejelenti a Hatóság honlapján – www.naih.hu – található Adatvédelmi Incidensbejelentő Rendszeren keresztül. Az Adatkezelő az adatvédelmi tisztviselő közreműködésével a bejelentéssel egyidejűleg kitölti 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 Hatóságot 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.

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

15. § (1) Az érintett jogait a GDPR III. fejezetének rendelkezései rögzítik. Az érintettnek joga van
a) átlátható tájékoztatáshoz,
b) 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) a tiltakozáshoz és arra, hogy ne terjedjen ki rá - a kizárólag automatizált adatkezelésen – ideértve a profilalkotást is – alapuló döntés hatálya (automatizált döntéshozatal egyedi ügyekben),
h) az adatvédelmi incidensről való tájékoztatáshoz.
(2) Az érintett jogosult az adatvédelmi tisztviselőhöz, a Hatósághoz (panasztétel joga), valamint a bírósághoz fordulni (jogorvoslati jogosultság).
16. § (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 nevén 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 joggyakorlásról jelen Utasítás 6. sz. melléklete szerinti nyilvántartást vezet.

7. Az adatkezelési tevékenységek nyilvántartása

17. § (1) Az Adatkezelő nyilvántartást vezet a feladat- és hatásköre alapján végzett adatkezelési tevékenységekről.
(2) Az Adatkezelő köteles a Hatósággal 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 előirányzott határidőt,
h) a technikai és szervezési intézkedések általános leírását.

(5) A GDPR 30. cikk (1) bekezdése szerinti adatkezelési nyilvántartás mintáját jelen Utasítás 7. számú melléklete tartalmazza.
(6) Az (5) bekezdés szerint készült nyilvántartást a szervezeti egységek vezetői az adatvédelmi tisztviselő közreműködésével készítik el, és a közös meghajtón kötelesek változás esetén, de legalább negyedévente (minden év március 15., június 15., szeptember 15., december 15. napjáig) a legfrissebb nyilvántartást menteni, a korábbi nyilvántartások egyidejű megtartásával.

8. Adattovábbítás, adattovábbítási nyilvántartás

18. § (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 adatának továbbításához.

(2) Az adatigénylés az adatvédelmi tisztviselő véleményének kikérést 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.

19. § (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 nyilvántartás elektronikus úton és papír alapon is lehet vezetni.
(3) Az adattovábbítási nyilvántartást jelen Utasítás 8. sz. melléklete tartalmazza.

9. Adattörlés, adattörlési nyilvántartás, megsemmisítési jegyzőkönyv

20. § (1) Az Adatkezelő indokolatlan késedelem nélkül köteles törölni az érintett személyes adatait, amennyiben az alábbi indok 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 jogi 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.

10. Adatfeldolgozó igénybevétele, adatfeldolgozói nyilvántartás

21. § (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 végzet 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.

11. Adatbiztonsági (technikai és szervezési) intézkedések

22. § (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 tűzfallal 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 vitte be 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 fájlletöltő (ide nem értve a vízügyi ágazat fájl letöltő szolgáltatását), játék-, csevegő-, szexuális szolgáltatásokat kínáló oldalak látogatása szigorúan tilos.
(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 és egyéb személyes adatokat tartalmazó iratokat biztonságosan, zárható páncélszekrényben elzárva kell tartani.
(12) Az Adatkezelő biztosítja az adatok és az adathordozó eszközök, iratok megfelelő fizikai védelmét.

12. Adatkezelő által kezelt közérdekű és közérdekből nyilvános adatok megismerése

23. § Az Adatkezelő által kezelt közérdekű és közérdekből nyilvános adatok megismerésére vonatkozó szabályokat az Országos Vízügyi Főigazgatóságnak és a vízügyi igazgatóságoknak a közérdekű adatok megismerésére és a szolgáltatási szerződés megkötésére vonatkozó eljárásrendjéről szóló főigazgatói utasítás tartalmazza.

13. Oktatás, vizsgáztatás

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

III. ZÁRÓ RENDELKEZÉSEK

25. § Jelen Utasítás 2023. október 16. napján lép hatályba, ezzel egyidejűleg hatályát veszti a 28/2021. (OVF) számú főigazgatói utasítás, valamint mellékletei.
26. § Jelen Utasítás felülvizsgálatáért és aktualizálásáért a Főigazgatói Hivatal vezetője felel. A felülvizsgálatot a jogszabályváltozást követő 30 napon belül, de legalább kétévente kell elvégezni.
27. § Jelen Utasításban foglaltakat a Főigazgatóság és a vízügyi igazgatóságok valamennyi foglalkoztatottja köteles megismerni és betartani.
28. § Jelen Utasításban foglaltak betartásáért a Főigazgató és az Igazgatók, valamint valamennyi szervezeti egység vezetője az általa irányított szervezeti egység vonatkozásában felelősséggel tartozik.
29. § A vízügyi igazgatóságok jelen Utasítás hatályba lépését követő 60 napon belül kötelesek felülvizsgálni és szükség szerint megalkotni az Igazgatóságukra vonatkozó részletszabályokat, amelyek nem lehetnek ellentétesek jelen Utasítás rendelkezéseivel.
30. § Jelen Utasítás mellékleteit az Adatkezelő köteles közzétenni honlapján, megfelelő fejléc alkalmazásával, letölthető formátumban.

Budapest, 2023. október 13.

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 nyilvántartása
9. sz. melléklet: Adattörlési nyilvántartás
10. sz. melléklet: Megsemmisítési jegyzőkönyv
11. sz. melléklet: Adatfeldolgozói nyilvántartás