Észak-dunántúli Vízügyi Igazgatóság
9021 Győr, Árpád út 28-32.

100- 9 /2013. Igazgatói Utasítás	**Tárgy: Adatvédelmi és adatbiztonsági szabályzat**

Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény 24. § (3) bekezdésében meghatározott felhatalmazás alapján, az Észak-dunántúli Vízügyi Igazgatóság (a továbbiakban: Igazgatóság) által kezelt személyes adatok védelme érdekében az alábbiak szerint intézkedem:

I. fejezet
Általános rendelkezések

A Szabályzat célja

1. Az Igazgatóság Adatvédelmi és adatbiztonsági szabályzatának (a továbbiakban: Szabályzat) célja, hogy az Igazgatóság tevékenysége során a személyes adatok védelméhez fűződő jog érvényesülésének biztosítása, illetve az Igazgatóság által kezelt személyes adatok jogosulatlan felhasználásának megakadályozása érdekében meghatározza a személyes adatok kezelése során irányadó adatvédelmi és adatbiztonsági előírásokat.

A Szabályzat hatálya

2. A Szabályzat hatálya kiterjed az Igazgatóság szervezeti egységeire, valamint a Igazgatóság személyi állománya által manuális módon kezelt adatokra. Az elektronikusan kezelt adatokra az Informatikai Biztonsági Szabályzatról szóló igazgatói utasítást kell alkalmazni.

A Szabályzat érvényesítése

3. A Szabályzat és szükség szerinti módosításának elkészítése az adatvédelmi felelős (a továbbiakban: adatvédelmi felelős) feladata.
4. A Szabályzatban előírtak betartatásáért a feladatkörében minden szervezeti egység vezetője felelős.
5. Az Igazgatóság személyi állománya feladatai ellátása során személyes adatot csak jogszabály (különösen az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.)) és közjogi szervezetszabályozó eszköz előírásainak figyelembevételével, az adatvédelemre vonatkozó alapelvek tiszteletben tartásával kezelhet.

Értelmező rendelkezések

6. Az Infotv. 3. §-ában meghatározott fogalmak irányadók a Szabályzat alkalmazása során.

II. fejezet
Az adatvédelem szervezeti rendszere

Az adatkezelő szerv vezetője

7. Az adatkezelő szerv vezetője az igazgató, aki felelős

a) az Igazgatóság adatvédelmi és adatbiztonsági intézményrendszerének kiépítéséért és működtetéséért, ennek keretében az Igazgatóság által kezelt személyes adatok védelméhez szükséges személyi, tárgyi és technikai feltételek biztosítását célzó, hatáskörébe tartozó intézkedések megtételéért,

b) az adatvédelmi oktatásért és továbbképzésért az adatvédelmi felelős bevonásával,

c) az Igazgatóság tevékenységének rendszeres adatvédelmi ellenőrzéséért, az ellenőrzés során esetlegesen feltárt hiányosságok vagy jogszabálysértő körülmények megszüntetéséért, a személyi felelősség megállapításához szükséges eljárás kezdeményezéséért, illetve lefolytatásáért,

d) az Infotv.-ben meghatározott jogainak gyakorlásához szükséges feltételek biztosításáért.

A belső adatvédelmi felelős

8. Az Igazgatóság adatvédelmi felelőse az Igazgatási és Jogi Osztály vezetője, aki rendelkezik az Infotv. 24. § (1) bekezdésben meghatározott végzettséggel.

9. Az adatvédelmi felelős az Igazgatóság adatvédelmi tevékenységének keretében

a) előkészíti az adatvédelem tárgyában kiadandó belső szabályzatok tervezetét, közreműködik az adatvédelmet érintő állásfoglalások kidolgozásában,

b) segíti az adatvédelmi tevékenységet, az egységes gyakorlat kialakítását,

c) közreműködik az adatkezelést érintő vizsgálatok lefolytatásában és az ezekkel összefüggő megkeresések megválaszolásában,

d) a Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: Hatóság) részére a jogszabályi előírások szerint tájékoztatást küld a megelőző évben elutasított személyes adat és közérdekű adat igényekről.

III. fejezet
A személyes adatok kezelése

Az adatkezelés elvei

10. Az érintettet az adatkezelő az adatkezeléshez történő hozzájárulásának beszerzése előtt tájékoztatja arról, hogy

a) mely adatait, milyen célból, milyen időtartamig jogosult kezelni az Igazgatóság;

b) mely szerv és hol végzi az adatkezelést, illetve az adatfeldolgozást;

c) az adatok továbbítására milyen célból és mely szervek részére kerülhet sor;

d) az adatkezeléssel kapcsolatban milyen jogokkal rendelkezik (tájékoztatáskérési, helyesbítési és törléskezdeményezési, valamint tiltakozási jog);

e) milyen jogorvoslati lehetőséggel rendelkezik (bírósági jogérvényesítés útja).

Az adatkezelések típusai

11. Az Igazgatóság – az adatkezelés eltérő célja alapján – ügyviteli, illetve nyilvántartási célú (adatállomány kialakítására irányuló) adatkezelést végez.

12. Az ügyvitelhez kapcsolódó adatkezelés kizárólag az ügy feldolgozásához kapcsolódik, alapvető célja az adott ügyhöz kapcsolódó eljárás lefolytatásához, az eljárás szereplőinek azonosításához és az ügy befejezéséhez szükséges adatok biztosítása. Az ügyviteli célú adatkezelés során a személyes adatok kizárólag az adott ügy irataiban és az ügyviteli segédletekben szerepelnek. Kezelésükre e célból csak az alapul szolgáló irat selejtezéséig van lehetőség.

13. A nyilvántartási célú adatkezelés az előre meghatározott szempontok alapján gyűjtött személyes adatfajtákból strukturált adatállományt hoz létre, az adatkezelés időtartama alatt biztosítva az adatok különböző jellemzők alapján történő visszakereshetőségét, automatizált nyilvántartások esetében a lekérdezhetőségét. Az egyes ügyekkel összefüggésben gyűjtött adatok kezelése ebben az esetben elválik az alapeljárástól, az adatok kezelésének időtartamát az adatok kezelésére felhatalmazást adó törvény vagy az érintett beleegyezésében foglaltak határozzák meg.

14. A nyilvántartási célú adatállomány kialakítását az adatvédelmi felelős állásfoglalása alapján az Igazgató írásban rendeli el.

Az érintett tájékoztatása

15. Az érintett tájékoztatást kérhet az Igazgatóságtól személyes adatai kezeléséről és kérheti személyes adatainak helyesbítését, illetve a jogszabályban elrendelt kötelező adatkezelések kivételével azok törlését, valamint – törvény felhatalmazása esetén – tiltakozhat személyes adatának kezelése ellen.

16. Az adatkezelő köteles az érintett személyes adatának kezelésével összefüggő kérelmére legkésőbb 30 – tiltakozási jog gyakorlása esetén 15 – napon belül írásban, közérthető formában választ adni, az Infotv. rendelkezései alapján.

17. Az érintett tájékoztatásának megtagadására az Infotv. 16. § (1) bekezdésében foglaltak alapján van lehetőség.

18. Ha törvény alapján az érintett tájékoztatása nem tagadható meg, a tájékoztatás kiterjed a kezelt adatok megjelölésére, az adatkezelés céljára, jogalapjára, időtartamára, az adatfeldolgozó nevére, címére és az adatkezeléssel összefüggő tevékenységére, továbbá arra, hogy kik és milyen célból kapják vagy kapták meg az adatokat.

19. A valóságnak nem megfelelő adatot az adatkezelő, ha a szükséges adatok rendelkezésre állnak, köteles helyesbíteni. Amennyiben a hibás adat nem helyesbíthető, akkor azt az Infotv. 17. § (2) bekezdése alapján, a 17. § (3) bekezdésében meghatározott kivételre figyelemmel törölni kell. A hibás adatot a kijavításig vagy a törlésig jelzéssel kell ellátni.

20. Az adat helyesbítéséről vagy törléséről az érintetten kívül mindazokat tájékoztatni kell, akiknek az adatot továbbították, kivéve, ha a tájékoztatás elmaradása az adatkezelés céljára tekintettel az érintett jogos érdekeit nem sérti. Ezen tájékoztatást a szervezeti egységek közvetlenül végzik, az adatvédelmi felelőst pedig a levél másolatának megküldésével tájékoztatják.

A tiltakozási jog gyakorlása

21. Az Infotv. 21. § (1) bekezdése szerinti adatkezelés elleni tiltakozás elbírálásának időtartamára – legfeljebb 15 napra – az adatkezelést az adott szervezeti egység vezetője felfüggeszti és erről az adatvédelmi felelőst tájékoztatja. A felfüggesztés időtartama alatt az adat a tiltakozási jog elbírásával összefüggő eljáráson kívül nem használható fel, nem továbbítható, a tárolásán kívül egyéb adatkezelési művelet nem végezhető.

22. Ha az adatzárolás közlésétől számított 30 napon belül az adatokhoz történő hozzájutás érdekében az érintett nem fordul bírósághoz vagy a bíróság az adatátadást kezdeményező

harmadik fél kérelmét elutasítja, az adatkezelő szervezeti egység köteles az érintett személyes adatát a határidő lejártától, illetve a döntés közlésétől számított 3 napon belül törölni.

Adattovábbítás és adatigénylés

23. Az Igazgatóság által kezelt adatokból személyes adatot továbbítani az érintett beleegyezésének hiányában csak törvényben meghatározott szerv vagy személy részére, törvényben meghatározott körben lehet, a célhoz kötöttség elvének maradéktalan érvényesítésével.

24. Az adattovábbítás jogszerű, ha a személyes adat birtokában lévő szerv vagy személy jogosult annak továbbítására, az adattovábbítás címzettje (adatkérő) pedig törvényi felhatalmazással vagy az érintett hozzájárulásával rendelkezik az adat kezeléséhez és az adatkérés célja mindezzel összhangban van. Az adattovábbítás feltételeinek megléte és a célhoz kötöttség a jogszerűség együttes követelménye.

25. Harmadik személy vagy szerv által benyújtott adattovábbítási kérelem elbírálása – a törvényben kötelezően előírt adattovábbítás esetét kivéve – az érintett szervezeti egység vezetőjének hatáskörébe tartozik. A szervezeti egység vezetője kikéri az adatvédelmi felelős állásfoglalását. Az adatigénylés abban az esetben teljesíthető, ha az tartalmazza

a) az adatigénylés célját, jogalapját (az alapul szolgáló törvényi rendelkezés pontos megjelölését);

b) a kért adatok körének pontos meghatározását;

c) az érintett személy azonosításához szükséges adatokat, több személyre vonatkozó adatigénylés esetén az érintettek azonosításához szükséges csoportképző ismérveket.

26. Az Igazgatóság – törvény eltérő rendelkezése hiányában – csak olyan személyes adatokat továbbíthat, amelyeknek az Igazgatóság a törvényben meghatározott adatkezelője. Amennyiben más szerv az adatkezelő, az adatkérést – törvény eltérő rendelkezése hiányában – el kell utasítani és az adatkérőt tájékoztatni kell arról, hogy a kért adatokat mely szervtől igényelheti.

27. Az adattovábbítás történhet kérelemre vagy törvény ilyen tartalmú rendelkezése alapján automatikusan, illetve a hozzáférés biztosítható kérelem alapján történő egyedi adatszolgáltatással, vagy számítógépes (online) lekérdezés lehetővé tételével.

28. A külföldre történő adattovábbítás során a személyes adatok megfelelő szintű védelme akkor biztosított, ha érvényesülnek az Infotv. 8. §-ában foglaltak.

Adattovábbítási nyilvántartás

29. Az Igazgatóság által kezelt személyes adatok továbbításáról az érintett szervezeti egységnél adattovábbítási nyilvántartást kell vezetni az Infotv. rendelkezései szerint.

Személyes adat kezelésének nyilvántartásba vétele

30. Az adatvédelmi felelős a személyes adat kezelés nyilvántartásba vételét kéri a Hatóságtól az adatkezelés megkezdése előtt legalább 30 nappal. A kötelező adatkezelés és az Infotv. 68. § (2) bekezdésében foglalt eset kivételével az adatkezelés nem kezdhető meg.

31. Az adatvédelmi felelős kötelező adatkezelés nyilvántartásba vételét az adatkezelést elrendelő jogszabály hatálybalépését követő 20 napon belül kérelmezi a Hatóságnál.

32. Nem kell bejelenteni az Infotv. 65. § (3) bekezdésben meghatározott adatkezeléseket.

33. A Hatóság a nyilvántartásába vételkor az adatkezelésnek nyilvántartási számot ad, amelyet az adatvédelmi felelős írásban közöl az érintett szervezeti egység vezetőjével. A

nyilvántartási számot az adatok harmadik személy részére történő továbbításánál, nyilvánosságra hozatalánál és az érintettnek történő kiadásánál fel kell tüntetni.

IV. fejezet
Adatbiztonsági előírások

Adatbiztonsági fokozatba történő besorolás

34. Az adatbiztonsági intézkedések meghatározása érdekében az Igazgatóság kezelésében lévő minden egyes adatállományt a védelmi igény szempontjából értékelni kell. Az értékelést és besorolást az a szervezeti egység vezetője készíti, ahol az adat keletkezik. Az adatállományt az alábbi biztonsági fokozatok valamelyikébe kell sorolni:

a) alapbiztonsági fokozat: azon adatkezelések tartoznak ebbe a fokozatba, amelyekben feldolgozott személyes adatokat törvény nyilvánossá minősítette, valamint amelyek egyedi azonosításra alkalmas személyes adatokat nem tartalmaznak és ezen adatok illetéktelen személy által történő megismerése, megváltoztatása, vagy törlése alapvetően nem veszélyezteti az Igazgatóság feladatainak végrehajtását és az érintett személyiségi jogainak érvényesülését. A megsérült, vagy megsemmisült adatok helyreállítása viszonylag kis ráfordítással, jelentős érdeksérelem nélkül elvégezhető,

b) fokozott biztonsági fokozat: azon adatkezelések tartoznak ebbe a fokozatba, amelyekben feldolgozott adatok illetéktelen személy által történő megismerése, megváltoztatása, vagy megsemmisítése veszélyezteti az Igazgatóság feladatainak végrehajtását, illetve az érintett személyiségi jogainak érvényesülését, a várható kár hatása túlmutat az igazgatósági érdekeken, hátrányosan befolyásolhatja az Igazgatóság adatszolgáltatási tevékenységét. A megsérült, vagy megsemmisült adatok helyreállítása nem, vagy csak jelentős anyagi, technikai ráfordítással valósítható meg,

c) kiemelt biztonsági fokozat: ebbe a fokozatba tartoznak azon adatkezelések, amelyek illetéktelen személy által történő megismerése, nyilvánosságra hozatala, illetve az adatok megváltoztatása, megsemmisülése az Igazgatóság – illetve más állami szerv – feladatainak ellátását lehetetlenné teszi, a nemzetközi kapcsolatokat, esetleg az érintett személyét veszélyeztetheti. A megsérült, vagy megsemmisült adatok helyreállítása nem, vagy csak aránytalan anyagi, technikai ráfordítással valósítható meg.

35. Az egyes adatkezelések biztonsági fokozatának megállapításához az 1. számú mellékletben meghatározott adatbiztonságot veszélyeztető kockázati elemeket kell figyelembe venni.

Az adatkezelés dokumentációjának védelméhez kapcsolódó adatbiztonsági intézkedések

36. A fokozott és kiemelt biztonsági fokozatba sorolt adatkezelések dokumentációit lehetőleg páncélszekrényben vagy biztonsági zárral ellátott lemezszekrényben, vagy biztonsági zárral, vasráccsal és lakattal, illetve behatolás elleni elektronikus védelemmel ellátott helyiségben kell őrizni.

V. fejezet
Ellenőrzés

Az adatkezelési ellenőrzésre jogosult személyek

37. Adatkezelési ellenőrzésre jogosult

a) az igazgató

b) az adatvédelmi felelős,

c) az érintett szervezeti egység vezetője az irányítása alá tartozó egység vonatkozásában, illetve az általa ellenőrzésre írásban kijelölt személy,

d) felettes szerv képviselője, valamint

e) jogszabályban erre felhatalmazott személy.

38. Az ellenőrzésre feljogosított az ellenőrzés céljára figyelemmel 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 adatkezelési tevékenységgel összefügg.

39. Az ellenőrzés során feltárt hiányosságokról, esetleges jogszabály- vagy normasértésekről az ellenőrzést végző az ellenőrzés befejezését követően írásban köteles tájékoztatni az adatvédelmi felelőst és az igazgatót, aki köteles haladéktalanul megtenni a jogszerű állapot helyreállításához szükséges intézkedéseket, illetve indokolt esetben elrendeli vagy kezdeményezi a személyi felelősség megállapításához szükséges eljárás lefolytatását.

VI. fejezet
Záró rendelkezések

40. Jelen Szabályzat **2013. április 01.** napján lép hatályba.

Győr, 2013. március 25.

Észak-dunántúli Vízügyi Igazgatóság 3. Győr

Németh József
igazgató

1.számú melléklet

Az adatbiztonságot veszélyeztető főbb kockázati elemek

1. A külső fenyegető tényezők:
a) természeti katasztrófa;
b) külső személy által elkövetett erőszakos cselekmény;
c) közműellátási zavarok;
d) külső személy tartózkodása az igazgatósági objektumban;
e) védelmi berendezések technikai hibája, vészhelyzet (pl. rövidzárlat, tűz, csőtörés).
2. A hardver eszközök fenyegetettsége:
a) műszaki jellegű hibák, rendellenességek;
b) káros környezeti hatás (feszültségingadozás, szennyeződés, elektromágneses sugárzás, elektrosztatikus feltöltődés);
c) a berendezések kezelésével, karbantartásával kapcsolatos hibák;
d) perifériákhoz való illetéktelen hozzáférés;
e) a berendezések manipulálása, rongálása, lopás;
f) az eszköz elhelyezésére szolgáló helyiség vagy munkahely helytelen kiválasztása.
3. Az adathordozók veszélyeztetettsége:
a) gyártási hiba;
b) károsodás nem szabályszerű tárolás, vagy kezelés miatt;
c) ismeretlen, vagy kétes eredetű adathordozó alkalmazása;
d) kontroll nélküli hozzáférés az adathordozókhoz, másolás;
e) saját adathordozó ellenőrzés nélküli alkalmazása szolgálati vagy magáncélra (vírusveszély, illegális másolás).
4. Az iratokhoz, informatikai dokumentációkhoz kapcsolódó kockázati elemek:
a) a rendszerdokumentáció teljes vagy részleges hiánya;
b) az iratok követhető rendszerezettségének hiánya;
c) az aktualitás hiánya;
d) jogosulatlan, hibás, ismeretlen eredetű változtatás;
e) kontroll nélküli hozzáférés, sokszorosítás.
5. A szoftverekhez kapcsolódó veszélyforrások:
a) nem jogtiszta, ismeretlen szoftver alkalmazása;
b) szoftverhiba;
c) jogosulatlan hozzáférés, másolás lehetősége;
d) szoftver ellenőrizetlen bevitele az informatikai rendszerbe;
e) vírusveszély;
f) szándékos vagy gondatlan kezelési, karbantartási hiba;
g) a szoftver sérülése, károsodása hardver hiba miatt;
h) dokumentációk hiánya, sérülése.
6. Az alkalmazói tevékenységgel, adatokkal összefüggő kockázati elemek:
a) adatvesztés, károsodás hardver vagy szoftver hiba miatt;
b) teljes, vagy részleges adatvesztés hibás adathordozó miatt;
c) a jogosult adatkezelő által szándékosan vagy tévedésből végzett adattörlés, – módosítás;
d) jogosulatlan adatkezelő által végzett másolás, törlés, módosítás;
e) hibás adatkezelés ismerethiány miatt;
f) kezelési előírások, oktatás hiánya.
7. Fenyegető tényezők a kommunikáció területén:
a) jogosulatlanok bejutása a hálózatba nem ellenőrizhető csatlakozás révén;

b) hálózati hardverek és szoftverek szándékos vagy gondatlan manipulálása;
c) adatforgalom lehallgatása;
d) váratlan forgalmazási akadályok, az átvitelt zavaró befolyások;
e) üzenetvesztés, üzenet megváltoztatása;
f) az adatátviteli eszközök sérülése, károsodása.
8. Személyhez fűződő veszélyforrások:
a) hibás adatkezelés ismerethiány vagy fáradtság, figyelmetlenség miatt;
b) az adatkezelésre vonatkozó előírások figyelmen kívül hagyása hiányos „biztonságtudat" miatt, a fenyegetettség lebecsülése;
c) szándékosan hibás adatkezelés belső késztetés vagy külső ráhatás következményeként;
d) jogosulatlan hozzáférés;
e) az ellenőrzés hiánya.