

## **19/2018. számú igazgatói utasítás az Adatvédelmi Szabályzatról**

A Tiszántúli Vízügyi Igazgatóság 2018. január 1. napján hatályba lépett Szervezeti és Működési Szabályzata (SZMSZ) alapján 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 Tanács 2016/679 számú rendelete (GDPR) 24. cikk (2) bekezdésében, valamint az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény 30. § (6) bekezdésében meghatározottak végrehajtása érdekében az alábbi utasítást adom ki:

### ***I. FEJEZET ÁLTALÁNOS RENDELKEZÉSEK***

#### **1. A szabályzat hatálya**

1.1. A szabályzat személyi hatálya kiterjed az igazgatóság közalkalmazotti jogviszonyban álló közalkalmazottaira, az igazgatóságnál foglalkoztatott munkavállalókra, továbbá a megbízási szerződéssel foglalkoztatottakra.

1.2. A szabályzat tárgyi hatálya kiterjed – az adatkezelési módszertől függetlenül – az igazgatóságnál folyó valamennyi ügyintézési és ügyirat-kezelési eljárásra.

1.3. Az igazgatóság ügyirat-kezelési eljárásra az iratkezelési szabályzat rendelkezései, a közérdekű adatok közzétételére a közérdekű adatok közzétételi kötelezettségének teljesítéséről szóló szabályzat rendelkezései, az adatvédelem informatikai előírásaira az Informatikai Biztonsági Szabályzat rendelkezéseit kell alkalmazni.

2. Az utasításban foglaltakat kell alkalmazni az adatkezelési műveletekre (megjelenési formától függetlenül, a megszerzéstől a törlésig).

#### **2. Alapelvek**

A személyes adatok:

- a) kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni („**jogszerűség, tisztességes eljárás és átláthatóság**”);
- b) gyűjtése csak meghatározott, egyértelmű és jogszerű célból történjen, és azokat ne kezeljék ezekkel a célokkal össze nem egyeztethető módon; nem minősül az eredeti céllal össze nem egyeztethetőnek a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból történő további adatkezelés („**célhoz kötöttség**”);
- c) az adatkezelés céljai szempontjából megfelelőek és relevánsak kell, hogy legyenek, és a szükségesre kell korlátozódniuk („**adattakarékosság**”);
- d) pontosnak és szükség esetén naprakésznek kell lenniük; minden észszerű intézkedést meg kell tenni annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul töröljék vagy helyesbítsék („**pontosság**”);
- e) tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé; a személyes adatok ennél hosszabb ideig történő tárolására csak akkor kerülhet sor, amennyiben a személyes adatok kezelésére közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy

statisztikai célból kerül majd sor, a rendeletben az érintettek jogainak és szabadságainak védelme érdekében előírt megfelelő technikai és szervezési intézkedések végrehajtására is figyelemmel („**korlátozott tárolhatóság**”);

f) kezelését oly módon kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve („**integritás és bizalmas jelleg**”).

Az adatkezelő felelős az (1) bekezdésnek való megfelelésért, továbbá képesnek kell lennie e megfelelés igazolására („**elszámoltathatóság**”).

A GDPR számos rendelkezése tekinthető úgy, mint olyan intézkedés, amely az elszámoltathatóság elvének konkrét megjelenése az adatkezelők tevékenysége során. E körbe sorolható különösen:

- a beépített és alapértelmezett adatvédelemre vonatkozó elvárásnak való megfelelés (25. cikk);
- a megfelelő adatfeldolgozók kiválasztása és igénybe vétele (28. cikk);
- az adatkezelési tevékenységek nyilvántartása (30. cikk);
- a megfelelő adatbiztonsági intézkedések megtétele (32. cikk);
- adatvédelmi incidensek megfelelő kezelése (33-34. cikk);
- az adatvédelmi hatásvizsgálat elvégzése (35. cikk);
- az adatvédelmi tisztviselő kijelölése (37. cikk);
- csatlakozás magatartási kódexhez (40. cikk);
- jóváhagyott tanúsítási mechanizmushoz való csatlakozás (42. cikk);
- a kötelező erejű vállalati szabályok alkalmazása adattovábbítás esetén (47. cikk).

g) Az adatkezelő a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével mind az adatkezelés módjának meghatározásakor, mind pedig az adatkezelés során olyan megfelelő technikai és szervezési intézkedéseket – például álnevesítést – hajt végre, amelyek célja egyrészt az adatvédelmi elvek, például az adattakarékosság hatékony megvalósítása, másrészt az e rendeletben foglalt követelmények teljesítéséhez és az érintettek jogainak védelméhez szükséges garanciák beépítése az adatkezelés folyamatába. („**Beépített, és alapértelmezett adatvédelem**”)

### 3. Értelmező rendelkezések

E szabályzat alkalmazása során:

1. *érintett*: bármely meghatározott, személyes adat alapján azonosított vagy - közvetlenül vagy közvetve - azonosítható természetes személy;

2. *személyes adat*: azonosított vagy azonosítható természetes személyre („érintett”) vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható;

3. *különleges adat*:

a) a faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviselői szervezeti tagságra, a szexuális életre vonatkozó személyes adat,

b) az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat, valamint a bűnügyi személyes adat;

4. *bűnügyi személyes adat*: a büntetőeljárás során vagy azt megelőzően a bűncselekménnyel vagy a büntetőeljárással összefüggésben, a büntetőeljárás lefolytatására, illetve a bűncselekmények felderítésére jogosult szerveknél, továbbá a büntetés-végrehajtás szervezeténél keletkezett, az érintettel kapcsolatba hozható, valamint a büntetett előéletre vonatkozó személyes adat;
5. *közérdekű adat*: az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő és tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől, így különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre, annak eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat;
6. *közérdekből nyilvános adat*: a közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli;
7. *az érintett hozzájárulása*: az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez;
8. *tiltakozás*: az érintett nyilatkozata, amellyel személyes adatainak kezelését kifogásolja, és az adatkezelés megszüntetését, illetve a kezelt adatok törlését kéri;
9. *adatkezelő*: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza; ha az adatkezelés céljait és eszközeit az uniós vagy a tagállami jog határozza meg, az adatkezelőt vagy az adatkezelő kijelölésére vonatkozó különös szempontokat az uniós vagy a tagállami jog is meghatározhatja;
10. *adatkezelés*: a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés;
11. *adattovábbítás*: az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele;
12. *nyilvánosságra hozatal*: az adat bárki számára történő hozzáférhetővé tétele;
13. *adattörlés*: az adatok felismerhetetlenné tétele oly módon, hogy a helyreállításuk többé nem lehetséges;
14. *adatmegjelölés*: az adat azonosító jelzéssel ellátása annak megkülönböztetése céljából;
15. *adatárolás*: az adat azonosító jelzéssel ellátása további kezelésének végleges vagy meghatározott időre történő korlátozása céljából;
16. *adatmegsemmisítés*: az adatokat tartalmazó adathordozó teljes fizikai megsemmisítése;
17. *adatfeldolgozás*: az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől, feltéve hogy a technikai feladatot az adatokon végzik;
18. *adatfeldolgozó*: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel;
19. *adatfelelős*: az a közfeladatot ellátó szerv, amely az elektronikus úton kötelezően közzeendő közérdekű adatot előállította, illetve amelynek a működése során ez az adat keletkezett;

20. *adatközlő*: az a közfeladatot ellátó szerv, amely - ha az adatfelelős nem maga teszi közzé az adatot - az adatfelelős által hozzá eljuttatott adatait honlapon közzéteszi;
21. *adatállomány*: az egy nyilvántartásban kezelt adatok összessége;
22. *harmadik fél*: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely nem azonos az érintettel, az adatkezelővel, az adatfeldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére felhatalmazást kaptak;
23. *nyilvántartási rendszer*: a személyes adatok bármely módon – centralizált, decentralizált vagy funkcionális vagy földrajzi szempontok szerint – tagolt állománya, amely meghatározott ismérvek alapján hozzáférhető;
24. *adattvédelmi incidens*: a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi;
25. *adattvédelem*: az adatkezelés során érintett természetes személyek jogainak és érdekeinek védelmére és az adatkezelés során felmerülő eljárásokra vonatkozó szabályozások és eljárások;
26. *adattbiztonság*: Az adatkezelő köteles az adatkezelési műveleteket úgy megtervezni és végrehajtani, hogy a vonatkozó jogszabályok alkalmazása során biztosítsa az érintettek magánszférájának védelmét;
27. *adathordozó*: az elektronikus adatok tárolására szolgáló, beépített vagy cserélhető eszközök összefoglaló neve.

## **II. FEJEZET** **RÉSZLETES RENDELKEZÉSEK**

### **1. Az igazgatóság vezetőinek, alkalmazottainak feladatai**

#### **A TIVIZIG vezetője**

Ellátja a törvény által a hatáskörébe utalt feladatokat, ennek keretében:

- 1.1. Kiadja az adattvédelmi és adattbiztonsági szabályzatot.
- 1.2. Ellenőrzi az adatkezelést és adattvédelmet, valamint az informatikát érintő nyilvántartásokat a belső ellenőrzési vezető, osztályvezetők és egységvezetők útján.

#### **Osztályvezetők és egységvezetők**

- 1.3. Ellenőrzi az adat- és az adatszolgáltatási nyilvántartás naprakészségét.
- 1.4. Koordinálják az adott osztályon dolgozó adatkezelői tevékenységét.
- 1.5. Biztosítják az irányításuk alá tartozó szervezeti egységnél az adatkezelés és az adattvédelem rendjét.

#### **Igazgatási és Jogi Osztály osztályvezető**

- 1.6. Gondoskodik az adatkezelési és adattvédelmi szabályzat kiadásáról és karbantartásáról.
- 1.7. Ellenőrzi az adatkezelésre vonatkozó jogszabályok, valamint a belső adattvédelmi szabályzatok rendelkezéseinek összhangját.
- 1.8. Megkeresésre véleményezi az adatszolgáltatás iránti kérelmeket.

#### **Ügyintéző**

- 1.9. Kezeli a munkakörébe tartozó adatokat.
- 1.10. A jogszabály által felhatalmazott személynek vagy szervezetnek adatot szolgáltat.
- 1.11. Vezeti az adat-, valamint az adatszolgáltatási nyilvántartást.



1.12. Megőrzi a tudomására jutott adatot.

1.13. Gondoskodik arról, hogy az általa vezetett nyilvántartás adataihoz illetéktelen személy ne férhessen hozzá, ügyel a nyilvántartás biztonságos tárolására.

1.14. Betartja az adatkezelésre, adatvédelemre és az adatbiztonságra vonatkozó rendelkezéseket.

1.15. Haladéktalanul jelzi az informatikusoknak a számítástechnikai eszközök bármilyen meghibásodását.

1.16. A tudomására jutott minősített adatot csak feladatainak ellátására használhatja fel, nem hozhatja illetéktelen személyek tudomására, nem adhat ki vezetője engedélye nélkül semmilyen információt. Az adatkezelő köteles az illetéktelen adatkérő, illetve igénylő részére az adathozzáférés és felhasználás minden formáját megtagadni. Az adatkezelő tudomására jutott adatok kezeléséért személy szerinti felelősséggel tartozik.

1.17. Köteles a munkája során tudomására jutott üzleti titkot, valamint a munkáltatóra, illetve a tevékenységére vonatkozó alapvető fontosságú információkat megőrizni. Ezen túlmenően sem közölhet illetéktelen személlyel olyan adatot, amely munkaköre betöltésével összefüggésben jutott a tudomására, és amelynek közlése a munkáltatóra vagy más személyre hátrányos következménnyel járna. A titoktartás nem terjed ki a közérdekű adatok nyilvánosságára és a közérdekből nyilvános adatra vonatkozó, külön törvényben meghatározott adatszolgáltatási és tájékoztatási kötelezettségre.

## **2. Az adatvédelmi tisztviselő**

A Rendelet értelmében a közhatalmi és közfeladatot ellátó adatkezelők és adatfeldolgozók kötelesek adatvédelmi tisztviselőt kijelölni. Ez a kötelezettség a Tiszántúli Vízügyi Igazgatóságra is kiterjed.

A Rendelet alapján az adatvédelmi tisztviselő kulcsszereplő az adatkezelés folyamatában, így a kijelölését, jogállását és feladatait is részletesen szabályozza a jogszabály.

A Rendelet 37. cikk (5) bekezdése úgy rendelkezik, hogy az adatvédelmi tisztviselőt „szakmai rátermettség és különösen az adatvédelmi jog és gyakorlat szakértői szintű ismerete, valamint a 39. cikkben említett feladatok ellátására való alkalmasság alapján kell kijelölni”. A (97) preambulumbekzdés alapján a szakértői ismeretek szükséges szintjét az adatkezelő által végzett adatkezelés, valamint az általa kezelendő személyes adatok tekintetében megkövetelt védelem alapján kell meghatározni. Az adatvédelmi tisztviselő kulcsszerepet játszik a szervezeten belül az adatvédelmi kultúra előmozdításában, és elősegíti a GDPR alapvető, például az adatok kezelésére vonatkozó elvekre, az érintett jogaira, a beépített és alapértelmezett adatvédelemre, az adatkezelési tevékenységek nyilvántartására, az adatkezelés biztonságára, valamint az adatvédelmi incidens bejelentésére és arról való tájékoztatásra vonatkozó rendelkezéseinek végrehajtását.

A 37. cikk (7) bekezdése előírja, hogy az adatkezelő vagy az adatfeldolgozó közzéteszi az adatvédelmi tisztviselő elérhetőségét, és közli azokat a felügyeleti hatóságokkal. Az adatvédelmi tisztviselő neve és elérhetősége az intraneten, a belső telefonkönyvben és a szervezeti ábrákon is feltüntethető.

Az adatvédelmi tisztviselő jogállását alapvetően meghatározza, hogy a GDPR 38. cikke értelmében az adatkezelő és az adatfeldolgozó biztosítja, hogy az adatvédelmi tisztviselő „a személyes adatok védelmével kapcsolatos összes ügybe megfelelő módon és időben bekapcsolódjon”. Az igazgatóság ennek a követelménynek az alábbiak szerint tesz eleget:

- az adatvédelmi tisztviselőt rendszeresen meghívják a közép- és felsővezetés megbeszéléseire.
- az adatvédelmi vonatkozású döntések meghozatalakor ajánlott a részvétele. Minden releváns információt időben kell átadni az adatvédelmi tisztviselőnek annak érdekében, hogy megfelelő tanácsot adhasson.
- az adatvédelmi tisztviselő véleményét mindig kellő súllyal kell figyelembe venni. Nézetkülönbség esetén rögzíteni kell annak az okát, hogy miért nem az adatvédelmi tisztviselő tanácsa szerint járnak el.
- az adatvédelmi tisztviselővel haladéktalanul konzultálni kell, ha adatvédelmi vagy más incidens következett be.

Az adatvédelmi tisztviselő feladatai:

a) A GDPR-nak való megfelelés ellenőrzése

A megfelelés ellenőrzésére vonatkozó feladatai részeként az adatvédelmi tisztviselő:

- információt gyűjt az adatkezelési tevékenységek meghatározása érdekében;
- elemzi és ellenőrzi az adatkezelési tevékenységek megfelelőségét;
- tájékoztatást, szakmai tanácsadást nyújt és ajánlásokat bocsát ki az adatkezelő vagy az adatfeldolgozó részére.

A megfelelés ellenőrzése nem jelenti azt, hogy az adatvédelmi tisztviselő személyesen felelős a rendelkezések be nem tartásáért. A GDPR egyértelművé teszi, hogy nem az adatvédelmi tisztviselő, hanem az adatkezelő köteles „megfelelő technikai és szervezési intézkedéseket végrehajtani annak biztosítása és bizonyítása céljából, hogy a személyes adatok kezelése e rendelettel összhangban történik” (24. cikk (1) bekezdése). Az adatvédelmi rendelkezések betartása nem az adatvédelmi tisztviselő, hanem az adatkezelő szervezeti felelőssége.

b) adatvédelmi hatásvizsgálat segítése

A beépített adatvédelem elve értelmében a 35. cikk (2) bekezdése kifejezetten előírja, hogy az adatkezelő az adatvédelmi hatásvizsgálat elvégzésekor az adatvédelmi tisztviselő „szakmai tanácsát köteles kikérni”. A 39. cikk (1) bekezdésének c) pontja pedig azt a feladatot írja elő az adatvédelmi tisztviselő részére, hogy „kérésre szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, valamint nyomon követi a hatásvizsgálat 35. cikk szerinti elvégzését”. Az adatvédelmi tisztviselő szakmai tanácsát különösen az alábbi kérdésekben kell kikérni:

- kell-e adatvédelmi hatásvizsgálatot végezni;
- milyen módszereket kell követni az adatvédelmi hatásvizsgálat elvégzésekor;
- az adatvédelmi hatásvizsgálatot szervezeten belül végezzék-e el, vagy kiszervezzék-e azt;
- milyen biztosítékokat (beleértve a technikai és szervezési intézkedéseket) kell alkalmazni az érintettek jogait és érdekeit érintő kockázatok enyhítésére;
- az adatvédelmi hatásvizsgálatot megfelelően végezték-e el, és a következtetései (lehet-e folytatni az adatkezelést, és milyen biztosítékokat kell alkalmazni), megfelelnek-e a GDPR-nek.

### **3. A hozzájáruláson alapuló adatkezeléshez kapcsolódó elvárások**

A Rendelet szerint az adatkezelés jogszerű, ha az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez. Az érintett hozzájárulása akkor megfelelő, ha az az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű

kinyilvánítása, amellyel az érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez. A hozzájárulásnak aktív cselekménynek kell lennie.

Személyes adat tehát elsődlegesen akkor kezelhető, ha ahhoz az érintett – önkéntesen, megfelelő tájékoztatást követően, határozottan, félreérthetetlenül – hozzájárul. A hozzájárulás megadható szóban, írásban vagy ráutaló magatartással, de a hallgatás itt nem beleegyezés. Az érintettnek minden esetben tisztában kell lennie azzal a ténnyel, hogy hozzájárulását adta, valamint azzal, hogy azt milyen mértékben tette. Különleges adat kezelése esetén kizárólag írásban lehet az adatkezeléshez hozzájárulni. Az érintettet minderről előzetesen tájékoztatni kell egy adatkezelési tájékoztató keretében.

#### **4. Adatfeldolgozó igénybevételek szabályai**

A GDPR 4. cikk 2. pontja alapján az „adatkezelés”: a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés.

A GDPR szerint az adatfeldolgozás során végzett műveletek megegyeznek a GDPR 4. cikk 2. pontban meghatározott adatkezelési műveletekkel, amelyeket viszont az adatkezelő már nem a saját nevében, hanem az adatkezelő nevében végez.

Az adatfeldolgozó által végzett adatkezelést az uniós jog vagy tagállami jog alapján létrejött olyan – az adatkezelés tárgyát, időtartamát, jellegét és célját, a személyes adatok típusát, az érintettek kategóriáit, valamint az adatkezelő kötelezettségeit és jogait meghatározó –, írásba foglalt - ide értve az elektronikus formátumot is - szerződésnek vagy más jogi aktusnak kell szabályoznia, amely köti az adatfeldolgozót az adatkezelővel szemben. A szerződés vagy más jogi aktus különösen előírja, hogy az adatfeldolgozó:

- a) a személyes adatokat kizárólag az adatkezelő **írásbeli** utasításai alapján kezeli – beleértve a személyes adatoknak valamely harmadik ország vagy nemzetközi szervezet számára való továbbítását is –, kivéve akkor, ha az adatkezelést az adatfeldolgozóra alkalmazandó uniós vagy tagállami jog írja elő. Ebben az esetben erről a jogi előírásról az adatfeldolgozó az adatkezelőt az adatkezelést megelőzően értesíti, kivéve, ha az adatkezelő értesítését az adott jogszabály fontos közérdekből tiltja;
- b) biztosítja azt, hogy a személyes adatok kezelésére feljogosított személyek **titoktartási kötelezettséget** vállalnak vagy jogszabályon alapuló megfelelő titoktartási kötelezettség alatt állnak;
- c) meghozza a 32. cikkben előírt intézkedéseket; (**adatkezelés biztonságára vonatkozó intézkedések**)
- d) tiszteletben tartja a további adatfeldolgozó igénybevételeire vonatkozóan feltételeket; (vagyis, hogy csak az adatkezelő előzetesen írásban tett eseti vagy általános felhatalmazása alapján alkalmaz további adatkezelőt)
- e) az adatkezelés jellegének figyelembevételével megfelelő technikai és szervezési intézkedésekkel a lehetséges mértékben segíti az adatkezelőt abban, hogy teljesíteni tudja kötelezettségét az érintett jogainak gyakorlásához kapcsolódó kérelmek megválaszolása tekintetében;
- f) segíti az adatkezelőt az elszámoltathatóságot erősítő kötelezettségek teljesítésében, figyelembe

- véve az adatkezelés jellegét és az adatfeldolgozó rendelkezésére álló információkat;
- g) az adatkezelési szolgáltatás nyújtásának befejezését követően az adatkezelő döntése alapján minden személyes adatot töröl vagy visszajuttat az adatkezelőnek, és törli a meglévő másolatokat, kivéve, ha az uniós vagy a tagállami jog az személyes adatok tárolását írja elő;
- h) az adatkezelő rendelkezésére bocsát minden olyan információt, amely az e cikkben meghatározott kötelezettségek teljesítésének igazolásához szükséges, továbbá amely lehetővé teszi és elősegíti az adatkezelő által vagy az általa megbízott más ellenőr által végzett auditokat, beleértve a helyszíni vizsgálatokat is.

Az adatfeldolgozó csak olyan további adatfeldolgozót vehet igénybe, amely vagy aki megfelelő garanciát nyújt az adatkezelés e rendelet követelményeinek való megfelelését és az érintett jogainak védelmét biztosító, megfelelő technikai és szervezési intézkedések végrehajtására.

Az adatfeldolgozó az adatkezelő írásbeli eseti vagy általános felhatalmazása nélkül további adatfeldolgozót nem vehet igénybe. Amennyiben az adatkezelő általános felhatalmazása alapján az adatfeldolgozó további vagy másik adatfeldolgozót akar igénybe venni, akkor erről a szándékáról tájékoztatja az adatkezelőt, aki kifogást emelhet a tervezett változások ellen. Az adatfeldolgozó *csak konkrét* adatkezelési műveletek tekintetében vehet igénybe további adatfeldolgozót. A két adatfeldolgozó közötti jogviszonyt ugyanolyan írásbeli, az uniós jog vagy tagállami jog alapján létrejött szerződés vagy más jogi aktus útján kell szabályozni, mint amilyen az adatkezelő és a megbízó adatfeldolgozó között létrejött.

A további adatfeldolgozóra is a megbízó adatfeldolgozóra vonatkozó adatvédelmi kötelezettségek vonatkoznak. Amennyiben a további adatfeldolgozó az adatvédelmi kötelezettségeit nem teljesíti, akkor az őt megbízó adatfeldolgozó teljes felelősséggel tartozik az adatkezelő felé a további adatfeldolgozó kötelezettségeinek teljesítéséért.

## **5. Az adatvédelmi hatásvizsgálat lefolytatása és az előzetes konzultáció kezdeményezése**

### *Adatvédelmi hatásvizsgálat*

A természetes személyek jogaira és szabadságaira nézve magas kockázattal járó esetekben az igazgatóság, mint adatkezelő – annak érdekében, hogy az adatkezelés jellegét, hatókörét, körülményeit és céljait, valamint a kockázat forrásait figyelembe véve felmérje a magas kockázat különös valószínűségét és súlyosságát – az adatkezelést megelőzően adatvédelmi hatásvizsgálatot végez.

Az adatvédelmi hatásvizsgálat célja az adatkezelés jellegének feltárása, szükségességének és arányosságának vizsgálata, valamint a személyes adatok kezeléséből eredően a természetes személyek jogait és szabadságait érintő kockázatok kezelésének elősegítése e kockázatok értékelésével és a kezelésükre szolgáló intézkedések meghatározásával.

Az adatvédelmi hatásvizsgálatot akkor kell elvégezni, ha az adatkezelés valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve. Az igazgatóság adatvagyon leltárának elkészítésekor minden szervezeti egység mérlegeli, hogy a fenti meghatározás alapján szükséges-e elvégezni a hatásvizsgálatot. A hatásvizsgálat során ki kell kérni adatvédelmi tisztviselő, továbbá az érintettek vagy képviselőik véleményét.

A hatásvizsgálat megállapításait folyamatosan felül kell vizsgálni és rendszeresen újra kell értékelni, különösen az adatkezelési műveletek által jelentett kockázat változása esetén.

Az adatvédelmi hatásvizsgálat alapvető jellemzői:

- a tervezett adatkezelési műveletek módszeres leírása és az adatkezelés céljainak ismertetése;
- az adatkezelési műveletek szükségességi és arányossági vizsgálata;
- az érintett jogait és szabadságait érintő kockázatok vizsgálata;
- a kockázatok kezelését célzó intézkedések bemutatása.



### *Előzetes konzultáció*

Ha a Rendelet 35. cikkében előírt adatvédelmi hatásvizsgálat megállapítja, hogy az adatkezelés az adatkezelő által a kockázat mérséklése céljából tett intézkedések hiányában valószínűsíthetően magas kockázattal jár, a személyes adatok kezelését megelőzően az igazgatóság konzultál a Nemzeti Adatvédelmi és Információszabadság Hatósággal. Ha a Hatóság véleménye szerint a tervezett adatkezelés megsértene a Rendeletet, a Hatóság legkésőbb a konzultáció iránti megkeresés kézhezvételétől számított nyolc héten belül írásban tanácsot ad.

Ez a határidő – a tervezett adatkezelés összetettségétől függően – hat héttel meghosszabbítható. A felügyeleti hatóság a megkeresés kézhezvételétől számított egy hónapon belül tájékoztatja az adatkezelőt vagy adott esetben az adatfeldolgozót a meghosszabbításról és a késedelem okairól. Az említett időtartamok felfüggeszthetők arra az időtartamra, amíg a Nemzeti Adatvédelmi és Információszabadság Hatóság nem jut hozzá azokhoz az információkhoz, amelyeket adott esetben a konzultáció céljából kért. Az igazgatóság a konzultáció során a Hatóságot tájékoztatja a 35. cikk (3) bekezdésében foglaltakról.

### **6. Az (elektronikus) adatvédelmi nyilvántartás**

Az általános adatvédelmi rendelet 30. cikke szerint az igazgatóság, mint adatkezelő kötelezettsége, hogy az általa végzett adatkezelési tevékenységekről nyilvántartást vezessen.

A nyilvántartás a következő információkat tartalmazza:

- a) az adatkezelő neve és elérhetősége, valamint – ha van ilyen – a közös adatkezelőnek, az adatkezelő képviselőjének és az adatvédelmi tisztviselőnek a neve és elérhetősége;
- b) az adatkezelés céljai;
- c) az érintettek kategóriáinak, valamint a személyes adatok kategóriáinak ismertetése;
- d) olyan címzettek kategóriái, akikkel a személyes adatokat közlik vagy közölni fogják, ideértve a harmadik országbeli címzetteket vagy nemzetközi szervezeteket;
- e) történik-e harmadik országba adattovábbítás
- f) a különböző adatkategóriák törlésére előírt határidők;
- g) technikai és szervezési intézkedések általános leírása.

Az igazgatóság megkeresés alapján köteles a nyilvántartást a Nemzeti Adatvédelmi és Információszabadság Hatóság rendelkezésére bocsátani.

### **7. Az adatigénylés során irányadó szabályok**

A közfeladatot ellátó szervek átláthatósága több pilléren nyugszik. Az egyik legfontosabb ezek közül az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) III. fejezetében szabályozott egyedi adatigénylés. Az Infotv. 3. § 5. pontja határozza meg a közérdekű adat fogalmát. A nyilvános adatok másik csoportjába a közérdekből nyilvános adatok tartoznak. Az Infotv. 3. § 6. pontja ebbe a körbe sorol a közérdekű adat fogalma alá nem tartozó minden olyan adatot, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli. Közérdekből nyilvános adatok ezért akár személyes adatok is lehetnek. A közérdekből nyilvános személyes adatok a célhoz kötöttség elvének tiszteletben tartásával terjeszthetők.

A közérdekű és közérdekből nyilvános adatok megismerésének részletszabályait külön igazgatói utasítás szabályozza.

### **8. Adattovábbítás a Tiszántúli Vízügyi Igazgatóság által kezelt személyes adatokból**

Az igazgatóság által kezelt személyes adatok továbbítása kizárólag a jogszabályban meghatározott feltételek fennállása esetén lehetséges. Az adattovábbítás jogszerűségét minden

esetben a tárgy szerint hatáskörrel rendelkező szervezeti egység vezetője köteles vizsgálni. A továbbított adatokról nyilvántartást kell vezetni.

### **9. Adattovábbítási nyilvántartás**

Az igazgatóság az adattovábbítás jogszerűségének ellenőrzése, valamint az érintett tájékoztatása céljából adattovábbítási nyilvántartást vezet, amely tartalmazza az általa kezelt személyes adatok továbbításának időpontját, az adattovábbítás jogalapját és címzettjét és a továbbított személyes adatok körének meghatározását.

### **10. Az érintettek jogai, valamint az érintettek jogainak érvényesítésével összefüggő feladatok**

Az érintettek főbb jogai a következők:

- *a rá vonatkozó személyes adatokhoz való hozzáférés;*

Az érintett hozzáférési jogának gyakorlása során az igazgatóság indokolatlan késedelem nélkül, de mindenféleképpen a kérelem beérkezésétől számított egy hónapon belül tájékoztatja az érintettet. Szükség esetén, figyelembe véve a kérelem összetettségét és a kérelmek számát, ez a határidő további két hónappal meghosszabbítható.

- *a helyesbítéshez való jog;*

Az igazgatóság késedelem nélkül köteles az érintett kérésére az érintettre vonatkozó pontatlan adatokat helyesbíteni.

- *a törléshez való jog („az elfeledtetéshez való jog”);*

Az igazgatóság késedelem nélkül köteles az érintett kérésére az érintettre vonatkozó személyes adatait törölni, amennyiben a Rendelet 17. cikk (1) bekezdésében felsorolt indokok valamelyike fennáll.

- *az adatkezelés korlátozásához való jog;*

A Rendelet 18. cikkében meghatározott feltételek fennállása esetén az érintett kérésére az igazgatóság korlátozza az adatkezelést.

- *tiltakozáshoz való jog;*

Amennyiben az érintett a saját helyzetével kapcsolatos okból tiltakozik a közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához, vagy az adatkezelő vagy 3. személy jogos érdekeinek érvényesítéséhez szükséges adatkezelés ellen, az igazgatóság az érintett adatait nem kezelheti tovább, kivéve, ha bizonyítja, hogy az adatkezelést olyan kényszerítő erejű jogos okok indokolják, amelyek előnyt élveznek az érintett jogaival és szabadságaival szemben, vagy amelyek jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódnak.

- *az adathordozhatósághoz való jog*

Az érintett jogosult arra, hogy a rá vonatkozó, általa egy adatkezelő rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja, továbbá jogosult arra, hogy ezeket az adatokat egy másik adatkezelőnek továbbítsa anélkül, hogy ezt akadályozná az az adatkezelő, amelynek a személyes adatokat a rendelkezésére bocsátotta, ha a Rendelet 20. cikkében foglalt feltételek fennállnak. Ebben az esetben az igazgatóság haladéktalanul gondoskodik arról, hogy az érintett személyes adatait tagolt, széles körben használt, géppel olvasható formátumban az érintett részére átadja.

Ha az érintettre vonatkozó személyes adatokat az érintettől gyűjtik, az igazgatóság a Rendelet 13. cikkében meghatározott információkat az érintett rendelkezésére bocsátja.

### **11. Az adatvédelmi incidenskezelési eljárásrend**

Adatvédelmi incidensnek minősül a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését,

megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi.

Az adatvédelmi incidens megfelelő és kellő idejű intézkedés hiányában fizikai, vagyoni vagy nem vagyoni károkat okozhat a természetes személyeknek, többek között

- a személyes adataik feletti rendelkezés elvesztését vagy a jogaik korlátozását,
- a hátrányos megkülönböztetést,
- a személyazonosság-lopást vagy a személyazonossággal való visszaélést,
- a pénzügyi veszteséget,
- az álnevesítés engedély nélküli feloldását,
- a jó hírnév sérelmét,
- a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülését, illetve
- a szóban forgó természetes személyeket sújtó egyéb jelentős gazdasági vagy szociális hátrányt.

Az adatvédelmi incidensek súlyos következményekkel járhatnak az érintettekre nézve, így ha megelőzni nem sikerül ezeket, fontos, hogy nagyon rövid határidőn belül intézkedések történjenek az incidensek következményeinek az elhárítása érdekében.

Az igazgatóság adatkezelésében és az adatfeldolgozónál bekövetkezett adatvédelmi incidens gyanúját észlelő személynek a tájékoztatást, amennyiben az elektronikus információbiztonság körében következett be, az információbiztonságáért felelős szervezeti egység vezetőjéhez kell megtenni, egyéb esetben a feladat és hatáskörrel rendelkező szervezeti egység vezetőjének kell jelezni.

Az igazgatósághoz külső észlelő személytől származó adatkezelésre vagy adatfeldolgozóra vonatkozó adatvédelmi incidens gyanújának tárgyában érkezett tájékoztatást haladéktalanul továbbítani kell a feladat és hatáskörrel rendelkező szervezeti egysége vezetője, vagy az információbiztonságért felelős szervezeti egység vezetőjének.

Az igazgatóságnál információbiztonságért felelős személy megvizsgálja, hogy

- a tájékoztatás alapján fennáll-e a gyanúja az adatvédelmi incidens bekövetkezésének,
- az adatvédelmi incidens az informatikai rendszert érintően következett-e be,
- mely szervezeti egységeket kell bevonni az intézkedések megtételére.

Az információbiztonságért felelős személy, amennyiben az informatikai rendszert érintően incidens gyanúja felmerül, döntés előkészítésére szolgáló anyagot megküldi az igazgatóság vezetője számára. Javaslatot tesz az incidens orvoslására, a tervezett intézkedésre.

Amennyiben nem az informatikai rendszert érintő incidens merül fel, az anyagot az információbiztonságért felelős személy haladéktalanul továbbítja a feladat és hatáskörrel rendelkező adatfeldolgozó releváns szervezeti egysége részére.

A feladat és hatáskörrel rendelkező szervezeti egysége kivizsgálja az adatvédelmi incidens súlyosságát. Amennyiben adatvédelmi incidens gyanúja felmerül, döntés előkészítésére szolgáló anyagot megküldi az igazgatóság vezetője számára. Javaslatot tesz az incidens orvoslására, a tervezett intézkedésre.

Az igazgatóság vezetője az adatvédelmi tisztviselő bevonásával jóváhagyja, illetve módosítja a javasolt intézkedéseket. Amennyiben az intézkedésnek anyagi vonzata van, az igazgató a döntésbe bevonja a gazdasági igazgató-helyettesét.

Az intézkedések végrehajtásáért az incidenssel érintett vezető felel. Az intézkedés végrehajtásról, annak lezárását követően beszámol az igazgatóság vezetőjének, és az adatvédelmi tisztviselőnek.

A megállapított adatvédelmi incidenst az igazgatóságnak a felügyeleti hatóság adatvédelmi incidens nyilvántartásába kell bejelenteni.

„Tudomásszerzésnek” az tekinthető, amikor az adatkezelő észszerű mértékű bizonyossággal rendelkezik arról, hogy olyan biztonsági esemény történt, amely személyes adatokkal kapcsolatos jogellenes műveletekhez vezethet.

Az adatkezelő azonnali vizsgálatot kezdeményez annak megállapítására, hogy történt-e adatvédelmi incidens, és ha igen, milyen intézkedések szükségesek, illetve szükség-e bejelentést tenni az adatvédelmi incidensről.

Ha az adatkezelő az elszámoltathatóság elvével összhangban bizonyítani tudja, hogy az adatvédelmi incidens valószínűsíthetően nem jár magas kockázattal a természetes személyek jogaira és szabadságaira nézve, akkor a bejelentés mellőzhető.

Az adatvédelmi incidenst az indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával a tudomásszerzést követően be kell jelenteni az illetékes felügyeleti hatóságnál.

A 72 órán túli bejelentéshez mellékelni kell a késedelem igazolására szolgáló indokokat is.

Amennyiben 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.

A felelős hatóság felé történő bejelentésnek tartalmaznia kell:

- az adatvédelmi tisztviselő (ha van) nevét és elérhetőségét,
- ismertetni kell az adatvédelmi incidens jellegét,
- az érintettek kategóriáit és hozzávetőleges számát,
- az incidenssel érintett adatok kategóriáit és hozzávetőleges számát,
- ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket,
- ismertetni kell az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket.

Az adatkezelő tájékoztatása alapján az adatvédelmi tisztviselő nyilvántartja az adatvédelmi incidenseket.

## **12. Ellenőrzés, közreműködés a Hatósággal**

A természetes személyek alapvető jogainak és szabadságainak a személyes adataik kezelése tekintetében történő védelme érdekében a vonatkozó szabályok alkalmazásának ellenőrzéséért egy független közhatalmi szerv (felügyeleti hatóság) felel. Ez a hatóság a Nemzeti Adatvédelmi és Információszabadság Hatóság.

Az adatkezelő és az adatfeldolgozó feladatai végrehajtása során a felügyeleti hatósággal – annak megkeresése alapján – együttműködik.

Az adatvédelmi tisztviselő feladta, hogy ellenőrizze, hogy az igazgatóság belső szabályzatai megfelelnek-e az adatvédelmi rendelkezéseknek. A megfelelés érdekében jelzi a belső szabályzat módosításának szükségességét az érintett egység vezetőjének, aki a módosítást a megadott határidőre köteles elvégezni.



Minden érintett jogosult arra, hogy panaszt tegyen egy felügyeleti hatóságnál, ha az érintett megítélése szerint a rá vonatkozó személyes adatok kezelése megsérti a vonatkozó előírásokat. Minden érintett hatékony bírósági jogorvoslatra jogosult, ha megítélése szerint a személyes adatainak nem megfelelő kezelése következtében megsértették a jogszabályban rögzített jogait. Az adatkezelőnek az adatvédelmi megfelelést ellenőrizni kell. A szabályoknak történő megfelelés érdekében a szervezetnél lévő adatbázist fel kell mérni. Ezen feladatot minden egységvezető 2018. május 25. napjáig elvégezte, az erről készült beszámolót az igazgatóság vezetőjének megküldte. A változásokat a szervezeti egység vezetője köteles lekövetni.

### **13. A Tiszántúli Vízügyi Igazgatóság által kezelt közérdekű és közérdekből nyilvános adatok megismerésével összefüggő szabályok**

A közérdekű és közérdekből nyilvános adatok megismerésének szabályait külön igazgatói utasítás szabályozza.

### **14. Oktatás, vizsgáztatás**

Az igazgatóságnak gondoskodni kell arról, hogy a személyes adatok kezelésére vonatkozó előírásokat a munkavállalók megismerjék. A fő szabályokat tartalmazó, valamint a munkaviszonnyal kapcsolatos adatkezelésről szóló tájékoztatót a dolgozók részére át kell adni, melynek igazolását tartalmazó dokumentum a személyi anyag része.

A vonatkozó szabályokról, a hatályba lépő új előírásokról a munkavállalókat folyamatosan tájékoztatni kell. A tájékoztatás formája lehet az adatvédelmi tisztviselő által az adatkezelési műveletekben részt vevő személyzet tudatosság-növelése érdekében tartandó képzés. A tájékoztatás módját az igazgatóság vezetője a bekövetkezett változások jellegére, súlyára tekintettel határozza meg az adatvédelmi tisztviselő javaslata alapján.

## **III. FEJEZET ZÁRÓ RENDELKEZÉSEK**

1. Jelen utasítás 2018. június 22. napján lép hatályba. Az utasítás hatálybalépésével egy időben a 14/2018. számú igazgatói utasítás hatályát veszti.
2. Elrendelem, hogy jelen igazgatói utasítás rendelkezései az utasítás hatálya alá tartozó közalkalmazottakkal kerüljenek megismertetésre, melynek tényét a megismerési záradék aláírásával dokumentálni kell.
3. Elrendelem továbbá, hogy az Igazgatási és Jogi Osztály az igazgatói utasítás aláírt digitális példányát haladéktalanul küldje meg az igazgatóság valamennyi szervezeti egysége, osztálya részére, valamint rögzítse azt az intraneten vezetett nyilvánartásba.

Debrecen, 2018. június 22.

