ORSZÁGOS VÍZÜGYI FŐIGAZGATÓSÁG

Hatályos:
2019. június 17.

Hatályon kívül helyezve:
66/2013. (OVF) számú főigazgatói utasítás I-II., valamint IV. fejezete, valamint annak mellékletei

Aktualizálás gyakorisága, rendje:
évente

Aktualizálásért felelős:
Főigazgatói Hivatal vezetője

Az OVF Főigazgatójának
21/2019. (OVF) számú
UTASÍTÁSA

törölt: .../

az Országos Vízügyi Főigazgatóság és a vízügyi igazgatóságok adatvédelmi és adatbiztonsági szabályzatáról

Az Országos Vízügyi Főigazgatóság (a továbbiakban: Főigazgatóság) Szervezeti és Működési Szabályzatáról szóló 7/2019. számú OVF Főigazgatói Utasítás 26. (3) bekezdésének felhatalmazása 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 (a továbbiakban: GDPR) 24. cikk (2) bekezdésében, valamint az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) 25/A. § (3) bekezdésében meghatározottak végrehajtása érdekében az alábbi utasítást (a továbbiakban: Szabályzat) adom ki:

I. ÁLTALÁNOS RENDELKEZÉSEK

1. A Szabályzat hatálya

1. § [A Szabályzat személyi hatálya]
A Szabályzat személyi hatálya az Adatkezelő közalkalmazottaira, munkavállalóira és közfoglalkoztatottjaira (a továbbiakban: foglalkoztatottak) terjed ki.

2. § [A Szabályzat tárgyi hatálya]
A Szabályzat tárgyi hatálya a Főigazgatóság és a vízügyi igazgatóságok (a továbbiakban együttesen: Adatkezelő) által folytatott minden olyan adatkezelésre kiterjed, amely természetes személy – manuális módon és elektronikusan kezelt – adataira vonatkozik. A Szabályzat rendelkezéseit a hazai és uniós jogszabályok adatkezelési műveletekre vonatkozó rendelkezéseit szem előtt tartva kell alkalmazni. Az elektronikusan kezelt személyes adatokra jelen Szabályzatot a vízügyi ágazat Informatikai Biztonsági Szabályzatával együttesen kell alkalmazni.

2. A Szabályzatban foglaltak alkalmazási köre

3. § [A Szabályzatban foglaltak alkalmazási köre]
A Szabályzatban 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.

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

3. Alapelvek

4. § [Az alapelvek szerepe]
A személyes adatok védelme és kezelése során az Adatkezelő foglalkoztatottjai az e cím alatt meghatározott alapelvek érvényre juttatásával kötelesek eljárni.

5. § [Átláthatóság elve]
A személyes adatok kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon végzi az Adatkezelő. Az Adatkezelő köteles a természetes személy adatainak kezelése során az adatgyűjtést, az adat felhasználását, a személyes adatokba való betekintést a természetes személy számára átlátható módon végezni. Az érintettnek joga van az Adatkezelő kilétéről történő tájékoztatásra. Az Adatkezelő adatkezelési tájékoztatóját jelen Szabályzat 4. számú melléklete tartalmazza.

6. § [Célhoz kötöttség elve]
Az Adatkezelő a személyes adatok gyűjtését kizárólag egyértelműen meghatározott, jogszerű célból végzi, és azokat nem kezeli ezekkel a célokkal össze nem egyeztethető módon. Az Adatkezelő által kezelt adatállományból kizárólag az Adatkezelő feladatkörének gyakorlása érdekében a célhoz kötöttség elvének szigorú érvényre juttatása mellett igényelhető és használható fel személyes adat. Személyes adat csak abban az esetben kezelhető, ha az adatkezelés célját egyéb eszközökkel célszerű módon nem lehetséges elérni.

7. § [Adattakarékosság elve]
A személyes adatoknak az adatkezelés céljai szempontjából megfelelőnek és relevánsnak kell lenniük, és a szükségesre kell korlátozódniuk.

8. § [Személyes adat törlésének elve]
(1) Az érintett kérésére az Adatkezelő haladéktalanul törli az érintettre vonatkozó személyes adatokat, ha az alábbi indokok valamelyike fennáll:
a) a személyes adatokra már nincs szükség abból a célból, amelyből azokat gyűjtötték vagy más módon kezelték;
b) az érintett visszavonja az adatkezelés alapját képező hozzájárulását, és az adatkezelésnek nincs más jogalapja;
c) az érintett a GDPR 21. cikk (1) bekezdése alapján tiltakozik az adatkezelése ellen, és nincs elsőbbséget élvező jogszerű ok az adatkezelésre, vagy az érintett a 21. cikk (2) bekezdése alapján tiltakozik az adatkezelés ellen;
d) a személyes adatokat jogellenesen kezelték – így különösen a Szabályzat az alapelvekkel ellentétes, az adatkezelés célja megszűnt vagy már nem szükséges;
e) a személyes adatokat az Adatkezelőre alkalmazandó uniós vagy tagállami jogban előírt jogi kötelezettség teljesítéséhez törölni kell.
(2) A személyes adat törlését az Adatkezelő megtagadja, amennyiben az adatkezelés szükséges:
a) a véleménynyilvánítás szabadságához és a tájékozódáshoz való jog gyakorlása céljából;
b) a személyes adatok kezelését előíró, az Adatkezelőre alkalmazandó uniós vagy tagállami jog szerinti kötelezettség teljesítése, illetve közérdekből végzett feladat végrehajtása céljából;
c) a GDPR 9. cikk (2) bekezdése h) és i) pontjának, valamint a 9. cikk (3) bekezdésének megfelelően a népegészségügy területét érintő közérdek alapján;
d) a GDPR 89. cikk (1) bekezdésével összhangban a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból, amennyiben az (1) bekezdésben említett jog valószínűsíthetően lehetetlenné tenné vagy komolyan veszélyeztetné ezt az adatkezelést; vagy
e) jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez.
(3) A GDPR 17. cikke szerinti adattörlési nyilvántartást jelen Szabályzat 5. számú melléklete tartalmazza.

9. § [Személyes adat helyesbítésének elve]

Az érintett jogosult arra, hogy

a) kérésére az Adatkezelő haladéktalanul helyesbítse a rá vonatkozó pontatlan személyes adatokat,
b) figyelembe véve az adatkezelés célját, kérje a hiányos személyes adatok kiegészítését.

10. § [Korlátozott tárolhatóság elve]

(1) A személyes adatok 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 a GDPR 89. cikk (1) bekezdésének megfelelően közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból kerül majd sor, a GDPR-ban az érintettek jogainak és szabadságainak védelme érdekében előírt megfelelő technikai és szervezési intézkedések végrehajtására is figyelemmel.

(2) Az adatkezelés időtartamára vonatkozó szabályokat jelen Szabályzat 4. számú melléklete rögzíti.

11. § [Az adatkezelés biztonságának elve]

Az Adatkezelő és az adatfeldolgozó a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja, ideértve, többek között, adott esetben:

a) a személyes adatok álnevesítését és titkosítását,
b) a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítását, integritását, rendelkezésre állását és ellenálló képességét,
c) fizikai vagy műszaki incidens esetén az arra való képességet, hogy a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását kellő időben vissza lehet állítani,
d) az adatkezelés biztonságának garantálására hozott technikai és szervezési intézkedések hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárást.

4. Az adatkezelés jogalapja

12. § [Az adatkezelés jogalapja]

(1) Személyes adat akkor kezelhető, ha

a) azt törvény elrendeli,
b) az a) pontban foglalt rendelkezés hiányában
   ba) az az Adatkezelő törvényben meghatározott feladatainak ellátásához feltétlenül szükséges és az érintett a személyes adatok kezeléséhez kifejezetten hozzájárult,
   bb) az az érintett vagy más személy létfontosságú érdekeinek védelméhez, valamint a személyek életét, testi épségét vagy javait fenyegető közvetlen veszély elhárításához vagy megelőzéséhez szükséges és azzal arányos, vagy
   bc) a személyes adatot az érintett kifejezetten nyilvánosságra hozta és az az adatkezelés céljának megvalósulásához szükséges és azzal arányos.

(2) Az (1) bekezdés a) pontjában, valamint a GDPR 6. cikk (1) bekezdés c) és e) pontjában meghatározott adatkezelés (a továbbiakban: kötelező adatkezelés) esetén a kezelendő adatok fajtáit, az adatkezelés célját és feltételeit, az adatok megismerhetőségét, az Adatkezelő személyét, valamint az adatkezelés időtartamát vagy szükségessége időszakos felülvizsgálatát az adatkezelést elrendelő törvény, illetve önkormányzati rendelet határozza meg.

5. Értelmező rendelkezések

13. § Jelen Szabályzat alkalmazásában:

(1) „Érintett”: bármely információ alapján azonosított vagy azonosítható természetes személy.

(2) „Személyes adat”: az érintettre vonatkozó bármely információ.
(3) „Adatkezelés”: az alkalmazott eljárástól függetlenül az adaton végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adat további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (például ujj- vagy tenyérlenyomat, DNS-minta, íriszkép) rögzítése.
(4) „Adatkezelés korlátozása”: a tárolt adat zárolása az adat további kezelésének korlátozása céljából történő megjelölése útján.
(5) „Adatbiztonság”: az adatbiztonság azokat a technikai módszereket foglalja magában, amelyek segítségével az adatvédelemben megfogalmazott alapelvek teljesíthetők. Az adatok jogosulatlan megszerzése, módosítása és tönkretétele elleni műszaki és szervezési intézkedések és eljárások együttes rendszere.
(6) „Adathordozó”: Olyan anyagi eszköz, közeg, amely alkalmas adatok megőrzésérem tárolására. Az adathordozó nem sértheti a GDPR 17. cikkét, azaz törléshez (feledéshez) való jogot.
(7) „Adatvédelem”: Az érintettre vonatkozó személyes adatok gyűjtésének, feldolgozásának, tárolásának és felhasználásának korlátozása, az érintett személyes adatainak védelme érdekében.
(8) „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 – különösen új technológiákat alkalmazó – típusa –, 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. Olyan egymáshoz hasonló típusú adatkezelési műveletek, amelyek egymáshoz hasonló magas kockázatokat jelentenek, egyetlen hatásvizsgálat keretei között is értékelhetőek.
(9) „Hozzáférési jogosultság”: Az informatikai feladatok ellátásáért felelős egység által beállított olyan jogosultság, melynek célja az informatikai eszköz erőforrásainak vagy magának az informatikai hálózatnak a védelme illetéktelen felhasználástól. A hozzáférési jogosultság határozza meg, hogy egy személynek vagy egy informatikai eszközön futó eljárásnak van-e lehetősége valamilyen objektum elérésére.
(10) „Álnevesítés”: személyes adat olyan módon történő kezelése, amely - a személyes adattól elkülönítve tárolt - további információ felhasználása nélkül megállapíthatatlanná teszi, hogy a személyes adat mely érintettre vonatkozik, valamint műszaki és szervezési intézkedések megtételével biztosítja, hogy azt azonosított vagy azonosítható természetes személyhez ne lehessen kapcsolni.
(11) „Profilalkotás”: személyes adat bármely olyan - automatizált módon történő - kezelése, amely az érintett személyes jellemzőinek, különösen a munkahelyi teljesítményéhez, gazdasági helyzetéhez, egészségi állapotához, személyes preferenciáihoz vagy érdeklődéséhez, megbízhatóságához, viselkedéséhez, tartózkodási helyéhez vagy mozgásához kapcsolódó jellemzőinek értékelésére, elemzésére vagy előrejelzésére irányul.
(12) „Nyilvántartási rendszer”: a személyes adatok bármely módon – centralizált, decentralizált vagy funkcionális vagy földrajzi szempontok szerint – tagolt állománya, amely meghatározott ismérvek alapján hozzáférhető.
(13) „Adatvédelmi nyilvántartás”: az Adatkezelő személyes adatokra vonatkozó adatkezeléseiről, az érintettek tájékozódásának elősegítése érdekében nyilvántartást vezet.

(14) „Elektronikus adatkezelési nyilvántartás”: az Adatkezelő által vezetett olyan nyilvántartás, mely tartalmazza az Adatkezelő nevét és elérhetőségeit, az adatvédelmi tisztviselő nevét és elérhetőségeit, az adatkezelés célját, az érintettek kategóriáit, a személyes adatok kategóriáit, a címzettek kategóriáit, az adattovábbítás tényét harmadik országba vagy nemzetközi szervezet részére, az adatok törlésére előirányzott határidőt és a technikai és szervezési intézkedések leírását az adatbiztonságot illetően.
(15) „Hozzájárulás” : az érintett akaratának önkéntes, határozott és megfelelő tájékoztatáson alapuló egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy az akaratát félreérthetetlenül kifejező más magatartás útján jelzi, hogy beleegyezését adja a rá vonatkozó személyes adatok kezeléséhez.
(16) „Adatkezelő”: az a foglalkoztatott (a Főigazgatóság esetében a Főigazgató és a vízügyi igazgatóság esetében az Igazgató), aki az adat kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja.
(17) „Adatfeldolgozó”: az a foglalkoztatott, aki az Adatkezelő megbízásából vagy rendelkezése alapján személyes adatokat kezel.
(18) Címzett: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely részére személyes adatot az Adatkezelő, illetve az adatfeldolgozó hozzáférhetővé tesz.
(19) „Harmadik személy”: olyan természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely nem azonos az érintettel, az Adatkezelővel, az adatfeldolgozóval vagy azokkal a személyekkel, akik az Adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére irányuló műveleteket végeznek.
(20) „Az érintett hozzájárulása”: az érintett akaratának önkéntes, határozott és megfelelő tájékoztatáson alapuló egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy az akaratát félreérthetetlenül kifejező más magatartás útján jelzi, hogy beleegyezését adja a rá vonatkozó személyes adatok kezeléséhez.
(21) „Adatvédelmi incidens”: az adatbiztonság olyan sérelme, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisülését, elvesztését, módosulását, jogosulatlan továbbítását vagy nyilvánosságra hozatalát, vagy az azokhoz való jogosulatlan hozzáférést eredményezi.
(22) „Felügyeleti hatóság”: a GDPR 51. cikkének megfelelően létrehozott független közhatalmi szerv részére megállapított feladat- és hatásköröket a Magyarország hatósága alá jogalanyok tekintetében a Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: Hatóság) gyakorolja.

II. RÉSZLETES RENDELKEZÉSEK

1. A Főigazgató és az Igazgató feladatai

14. § [Az Adatkezelő szerv vezetőjének feladatai]

A Főigazgató és az Igazgató feladata

a) a jogszabály által a feladat- és hatáskörbe utalt adatkezelési rendszerek egészének (nyilvántartások, adattárak, munkafolyamatok, információáramlások és feldolgozások, jogosultságok) kialakítása és irányítása, rendeltetésszerű működtetése,
b) gondoskodni a személyes adatok körében a jogosulatlan hozzáférés, közlés, megváltoztatás vagy törlés megelőzéséről, a technikai védelemről, továbbá az, 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,

c) személyes felelősséggel tartozik az általa vezetett szerv, illetve irányítása alá tartozó szervek tevékenységéért, azok törvényes és szakszerű működéséért, ezen belül az irányítása alatt álló állomány adatkezelői tevékenységéért, az adatvédelmi előírások, valamint a kapcsolódó ügyviteli és minősített adat – védelmi szabályok betartásáért,
d) a védelmi és biztonsági szabályok gyakorlati érvényesülésének ellenőrzése, intézkedés a hiányosságok felszámolására,
e) az adatkezelések szervezeti és működési feltételeinek kialakítása, gondoskodás a működési követelmények az adatbiztonsági követelmények érvényre juttatásáról,
f) az adatszolgáltatásokról vezetett nyilvántartás ellenőrzése,
g) adatvédelmi tisztviselő kijelölése vagy megbízása,
h) az adatvédelmi oktatás szabályainak jóváhagyása,
i) az adatvédelmi incidensek megelőzése, kezelése, bekövetkezéskor gyors és hatékony reagálásról történő intézkedés,
j) az adatvédelmi incidens bekövetkezésekor felelős az érintettek és a Hatóság tájékoztatásáért.

2. Az adatvédelmi tisztviselő és az adatvédelmi megbízott

15. § [Az adatvédelmi tisztviselő]

(1) Az adatvédelmi tisztviselő jogállása: 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 adatvédelmi tisztviselő feladatai különösen:

a) tájékoztat és szakmai tanácsot ad a foglalkoztatottak részére adatvédelmi kérdésekben,
b) ellenőrzi a GDPR-nak, az Infotv.-nek, valamint jelen Szabályzatnak való megfelelést, ideértve a feladatkörök kijelölését, az adatkezelési műveletekben résztvevő munkavállalók tudatosság – növelését és képzését, valamint a kapcsolódó auditokat is,
c) kérésre szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, valamint nyomon követi a hatásvizsgálat elvégzését,
d) együttműködik a Hatósággal,
e) az adatkezeléssel összefüggő ügyekben kapcsolattartó pontként szolgál a Hatóság felé, valamint adott esetben bármely egyéb kérdésben konzultációt folytat vele.

16. § [Az adatvédelmi megbízott]

(1) Az Adatkezelő jogosult adatvédelmi megbízottat igénybe venni, amennyiben jelen Szabályzat 15. §-ában meghatározott adatvédelmi tisztviselő kijelölése szervezeten belül nem lehetséges.

(2) Az adatvédelmi megbízott feladatai különösen:

a) Részt vesz az adatvédelmet érintő belső szabályzatok kidolgozásában, gondoskodik azok naprakészségéről, vezeti az adatkezelési nyilvántartást, részt vesz az Adatkezelő személyes adatok védelmével és közérdekű adatok nyilvánosságával kapcsolatos feladatainak ellátásában. Közreműködik, illetve segítséget nyújt az adatkezeléssel összefüggő döntések meghozatalában, valamint az érintettek jogainak biztosításában.

b) Kivizsgálja a hozzá érkezett bejelentéseket, jogosulatlan adatkezelés észlelése esetén annak megszüntetésére hívja fel az Adatkezelőt vagy az Adatfeldolgozót.
c) Felkérés alapján adatvédelmi szempontból véleményezi a Főigazgatói Utasításokat, illetve Szabályzatokat.
d) Megkeresésre véleményezi az adatszolgáltatás iránti kérelmeket.
e) Az adatvédelmi és az ezzel összefüggő adatbiztonsági feladatokról, az adatvédelemmel kapcsolatos problémákról, folyamatosan tájékoztatja a Főigazgatóság esetében a Főigazgatót, a vízügyi igazgatóság esetében az Igazgatót.
f) Javasolja és támogatja az adatvédelem, illetve az ahhoz kapcsolódó adatbiztonság területén kifejlesztett új technológiák és eszközök alkalmazását.

3. Az adatkezelés jogszerűségének biztosítása

17. § [A hozzájáruláson alapuló adatkezelés]

(1) Amennyiben az Adatkezelő hozzájáruláson alapuló adatkezelést kíván végezni, úgy az érintett hozzájárulását személyes adatai kezeléséhez jelen Szabályzat 1. számú melléklete szerinti adatkérő lap szerinti tartalommal és tájékoztatással kell kérni.
(2) Az érintettel az adatkezelés megkezdése előtt közölni kell, hogy az adatkezelés hozzájáruláson alapul vagy kötelező.
(3) Az érintettet az adatkezelés megkezdése előtt egyértelműen és részletesen tájékoztatni kell az adatai kezelésével kapcsolatos minden tényről, így különösen:
a) az adatkezelés céljáról és jogalapjáról,
b) az adatkezelésre és az adatfeldolgozásra jogosult személyéről,
c) az adatkezelés időtartamáról,
d) arról, ha az érintett személyes adatait az Adatkezelő az Infotv. 5. § b) pontja alapján kezeli,
e) arról, hogy kik ismerhetik meg az adatokat,
f) a tájékoztatásnak ki kell terjednie az érintett adatkezeléssel kapcsolatos jogaira és jogorvoslati lehetőségeire is,
g) arról, hogy az érintett a hozzájárulását bármikor visszavonhatja.
(4) A hozzájárulás visszavonása nem érinti a hozzájáruláson alapuló, a visszavonás előtti adatkezelés jogszerűségét. A hozzájárulás megadása előtt az érintettet erről tájékoztatni kell.
(5) Ha a hozzájáruláson alapuló adatkezelés célja az Adatkezelővel írásban kötött szerződés végrehajtása, a szerződésnek tartalmaznia kell minden olyan információt, amelyet a személyes adatok kezelése szempontjából – az Infotv. és a GDPR alapján – az érintettnek ismernie kell, így különösen a kezelendő adatok meghatározását, az adatkezelés időtartamát, a felhasználás célját, az adatok továbbításának tényét, címzettjeit, adatfeldolgozó igénybevételének tényét. A szerződésnek félreérthetetlen módon tartalmaznia kell, hogy az érintett aláírásával hozzájárul adatainak a szerződésben meghatározottak szerinti kezeléséhez.

18. § [Jogi kötelezettség teljesítésén alapuló adatkezelés]

(1) A jogi kötelezettségen alapuló adatkezelés esetén a kezelhető személyes adatok körére, az adatkezelés céljára, az adatok tárolásának időtartamára, a címzettekre az adatkezelés alapjául szolgáló jogszabályok rendelkezései irányadók.
(2) A jogi kötelezettség teljesítése jogcímén alapuló adatkezelés az érintett hozzájárulásától független, mivel az adatkezelést jogszabály határozza meg.

Az érintettel az adatkezelés megkezdése előtt ez esetben közölni kell, hogy az adatkezelés kötelező, továbbá az érintettet az adatkezelés megkezdése előtt egyértelműen és részletesen tájékoztatni kell az adatai kezelésével kapcsolatos minden tényről, így különösen az adatkezelés céljáról és jogalapjáról, az adatkezelésre és az adatfeldolgozásra jogosult személyéről, az adatkezelés időtartamáról, arról, ha az érintett személyes adatait az Adatkezelő a rá vonatkozó jogi kötelezettség alapján kezeli, illetve arról, hogy kik ismerhetik meg az adatokat. A tájékoztatásnak ki kell terjednie az érintett adatkezeléssel kapcsolatos jogaira és jogorvoslati lehetőségeire is.
Kötelező adatkezelés esetén a tájékoztatás megtörténhet az előbbi információkat tartalmazó jogszabályi rendelkezésekre való utalás nyilvánosságra hozatalával is.
(3) A részletszabályokat jelen Szabályzat 43-45. §-ai rögzítik.

19. § [Az Adatkezelő adatkezelési tájékoztatója]

(1) Az Adatkezelő általános adatkezelési tájékoztatóját jelen Szabályzat 4. számú melléklete tartalmazza.
(2) Az Adatkezelő valamennyi adatkezelése során köteles biztosítani az érintett jogainak gyakorlását.

4. Az adatvédelmi hatásvizsgálat lefolytatása

20. § [Az adatvédelmi hatásvizsgálat lefolytatása]

(1) Az Adatkezelő a GDPR 35. cikkében rögzített adatvédelmi hatásvizsgálat lefolytatását az adatvédelmi tisztviselő vagy az adatvédelmi megbízott szakmai tanácsa alapján végzi.
(2) A 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.
(3) 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 konzultálni köteles a Hatósággal.
(4) A hatásvizsgálat mintáját jelen Szabályzat 2. számú 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.

5. Az előzetes konzultáció

21. § [Az előzetes konzultáció]

(1) Az Adatkezelő jelen Szabályzat 19. § (3) bekezdése alapján a Hatósággal folytatott konzultáció során a Hatóságot tájékoztatja:
a) adott esetben az adatkezelésben részt vevő Adatkezelő, közös Adatkezelők és adatfeldolgozók feladatköreiről,
b) a tervezett adatkezelés céljairól és módjairól,
c) az érintettek a GDPR értelmében fennálló jogainak és szabadságainak védelmében hozott intézkedésekről és garanciákról,
d) az adatvédelmi tisztviselő vagy az adatvédelmi megbízott elérhetőségeiről,
e) az adatvédelmi hatásvizsgálatról és
f) a Hatóság által kért minden egyéb információról.
(2) Az Adatkezelő a konzultációt követően a Hatóság tanácsainak figyelembevételével jár el.

6. Az adatvédelmi incidensek kezelése

22. § [Az adatvédelmi incidensek kezelése]

(1) Az adatvédelmi incidenst az Adatkezelő indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, bejelenti a Hatóságnak, kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve.
Ha a bejelentés nem történik meg 72 órán belül, mellékelni kell hozzá a késedelem igazolására szolgáló indokokat is.

(2) 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.

(3) Amennyiben az Adatkezelő foglalkoztatottjai adatvédelmi incidenst észlelnek, haladéktalanul értesíteniük kell a Főigazgatóság esetében a Főigazgatót, a vízügyi igazgatóság esetében az Igazgatót, az Informatikai Főosztály vezetőjét és az információbiztonsági felelőst a szolgálati út betartásával.

(4) Adatvédelmi incidens bejelentése esetén a Főigazgatóság esetében a Főigazgató, a vízügyi igazgatóság esetében az Igazgató – az Informatikai Főosztály vezetőjének és az információbiztonsági felelős bevonásával – haladéktalanul a bejelentés megvizsgálásáról intézkedik, ennek során azonosítani kell az incidenst, el kell dönteni, hogy valódi incidensről, vagy téves riasztásról van szó. Meg kell vizsgálni és meg kell állapítani:
a) az incidens bekövetkezésének időpontját és helyét,
b) az incidens leírását, körülményeit, hatásait,
c) az incidens során kompromittálódott adatok körét, számosságát,
d) a kompromittálódott adatokkal érintett személyek körét,
e) az incidens elhárítása érdekében tett intézkedések leírását,
f) a kár megelőzése, elhárítása, csökkentése érdekében tett intézkedések leírását.

(5) Adatvédelmi incidens bejelentését az adatvédelmi tisztviselő vagy az adatvédelmi megbízott végzi el a Hatóság honlapján található iratminta alapján, jelen Szabályzat 3. számú mellékletének egyidejű kitöltésével.

(6) Adatvédelmi incidens bekövetkezése esetén az érintett rendszereket, személyeket, adatokat be kell határolni és el kell különíteni, valamint gondoskodni kell az incidens bekövetkezését alátámasztó bizonyítékok begyűjtéséről és megőrzéséről. Ezt követően lehet megkezdeni a károk helyreállítását és a jogszerű működés visszaállítását.

(7) Az informatikai rendszereken naplózni kell a hozzáféréseket és a hozzáférési kísérleteket, és ezeket folyamatosan elemezni kell.

(8) Az adatvédelmi incidensek eljárásrendjét jelen Szabályzat 8. számú melléklete rögzíti.

(9) Az adatvédelmi nyilvántartásban szereplő adatvédelmi incidensekre vonatkozó adatokat 5 évig meg kell őrizni.

7. Adatfeldolgozókra vonatkozó követelmények

23. § [Az adatfeldolgozó]

(1) Az Adatkezelő az adatok feldolgozásával kapcsolatos műveletek elvégzésére adatfeldolgozót vehet igénybe. Az adatfeldolgozónak a személyes adatok feldolgozásával kapcsolatos jogait és kötelezettségeit az Infotv., valamint az adatkezelésre vonatkozó külön törvények keretei között az adatkezelő határozza meg. Az adatfeldolgozásra vonatkozó megbízási szerződést írásba kell foglalni.

(2) Az Adatkezelő:
a) az adatkezelési műveletekre vonatkozó utasítások jogszerűségéért felel,
b) külső adatfeldolgozót vehet igénybe,
c) adatfeldolgozásra nem adhat megbízást olyan vállalkozásnak, amely a feldolgozandó személyes adatokat felhasználó üzleti tevékenységben érdekelt,
d) az igénybe vett adatfeldolgozó esetében szerződésben meghatározott szigorú szabályok szerint köteles eljárni, melyek betartásáról rendszeres ellenőrzéssel köteles meggyőződni (az ellenőrzést a szerződést aláíró vezetők végzik).

(3) Az adatfeldolgozó:
a) tevékenységi körén belül, illetőleg az Adatkezelő által meghatározott keretek között felelős a személyes adatok feldolgozásáért, megváltoztatásáért, törléséért, továbbításáért és nyilvánosságra hozataláért,
b) tevékenységének ellátása során más adatfeldolgozót az Adatkezelő rendelkezése szerint vehet igénybe,
c) az adatkezelést érintő érdemi döntést nem hozhat, a tudomására jutott személyes adatokat kizárólag az Adatkezelő rendelkezései szerint dolgozhatja fel, saját céljára adatfeldolgozást nem végezhet, továbbá a személyes adatokat az Adatkezelő rendelkezései szerint köteles tárolni és megőrizni.

8. Az adatvédelmi nyilvántartás

24. § [Az adatvédelmi nyilvántartás]

(1) Az Adatkezelő nyilvántartást vezet a 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 Szabályzatnak megfelelően úgy kell kialakítani és működtetni az adatvédelmi nyilvántartás feltételeit, hogy azok biztosítsák a jogosulatlan hozzáférés megakadályozását.
(4) Az adatvédelmi nyilvántartás tartalmazza:
a) az Adatkezelő nevét és elérhetőségét, az adatvédelmi tisztviselő nevét és elérhetőségét, az adatfeldolgozó nevét és elérhetőségét,
b) adatkezelés célját,
c) az adatkezelés jogalapját,
d) az érintettek körét,
e) az érintettekre vonatkozó adatok leírását,
f) az adatok forrását,
g) az adatok kezelésének időtartamát,
h) a továbbított adatok fajtáját, címzettjét és a továbbítás jogalapját,
i) a tényleges adatkezelés, illetve az adatfeldolgozás helyét és az adatfeldolgozónak az adatkezeléssel összefüggő tevékenységét,
j) az alkalmazott adatfeldolgozási technológia jellegét.
(5) A GDPR 30. cikk (1) bekezdése szerinti adatkezelési nyilvántartás mintáját jelen Szabályzat 6. számú melléklete tartalmazza.

9. Az adatigénylés során irányadó szabályok

25. § [Az adatigénylés]

(1) Az Adatkezelő által kezelt személyes adatokból kizárólag az Adatkezelő feladat- és hatáskörének gyakorlása érdekében, célhoz kötöttség elvének szigorú érvényre juttatása mellett igényelhető és használható fel személyes adat.

(2) A más adatkezelők által kezelt olyan adatállományokból, amelyekből történő adatigénylésre az Adatkezelő érintett adatkezelésre irányadó törvény felhatalmazza, csak az adott törvényben meghatározott feladat ellátása érdekében végezhető adatlekérdezés, azok harmadik személynek vagy szervnek nem továbbíthatók.

(3) Az érintett jogosult arra, hogy az Adatkezelőtől visszajelzést kapjon arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e, és ha ilyen adatkezelés folyamatban van, jogosult arra, hogy a személyes adatokhoz és a következő információkhoz hozzáférést kapjon:

a) az adatkezelés céljai,
b) az érintett személyes adatok kategóriái,
c) azon címzettek vagy címzettek kategóriái, akikkel, illetve amelyekkel a személyes adatokat közölték vagy közölni fogják, ideértve különösen a harmadik országbeli címzetteket, illetve a nemzetközi szervezeteket,
d) adott esetben a személyes adatok tárolásának tervezett időtartama, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjai,
e) az érintett azon joga, hogy kérelmezheti az Adatkezelőtől a rá vonatkozó személyes adatok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen,
f) a Hatósághoz címzett panasz benyújtásának joga,
g) ha az adatokat nem az érintettől gyűjtötték, a forrásukra vonatkozó minden elérhető információ,
h) a GDPR 22. cikk (1) és (4) bekezdésében említett automatizált döntéshozatal ténye, ideértve a profilalkotást is, valamint legalább ezekben az esetekben az alkalmazott logikára és arra vonatkozó érthető információk, hogy az ilyen adatkezelés milyen jelentőséggel bír, és az érintettre nézve milyen várható következményekkel jár.

(4) Ha személyes adatoknak harmadik országba vagy nemzetközi szervezet részére történő továbbítására kerül sor, az érintett jogosult arra, hogy tájékoztatást kapjon a továbbításra vonatkozóan a GDPR 46. cikk szerinti megfelelő garanciákról.

(5) Az Adatkezelő az adatkezelés tárgyát képező személyes adatok másolását az érintett rendelkezésére bocsátja. Az érintett által kért további másolatokért az Adatkezelő az adminisztratív költségeken alapuló, jogszabályban meghatározott mértékű díjat számíthat fel. Ha az érintett elektronikus úton nyújtotta be a kérelmet, az információkat széles körben használt elektronikus formátumban kell rendelkezésre bocsátani, kivéve, ha az érintett másként kéri. A másolat igénylésére vonatkozó jog nem érintheti hátrányosan mások jogait és szabadságait.

10. Adattovábbítás az Adatkezelő által kezelt személyes adatokból

26. § [Az adattovábbítás]

(1) Ha az érintett kifejezett hozzájárulását adta, az adatok továbbítását bizonyos körülmények esetén lehetővé kell tenni, ha az adattovábbítás alkalomszerű, és valamely szerződéssel vagy jogi igénnyel kapcsolatban válik szükségessé, függetlenül attól, hogy a szerződés teljesítésére vagy a jogi igény érvényesítésére bírósági eljárás, illetve közigazgatási vagy egyéb nem bírósági útra tartozó eljárás keretében kerül-e sor, ideértve a szabályozói szervek előtt zajló

eljárásokat is.

(2) Szintén lehetővé kell tenni az adatok továbbítását, ha azt az uniós vagy tagállami jogban megállapított fontos közérdek védelme megkívánja, vagy ha a továbbításra jogszabály alapján létrehozott nyilvántartásból kerül sor, és célja a nyilvánosság vagy az e tekintetben jogos érdekkel rendelkezők általi betekintés biztosítása.
Ez utóbbi esetben az ilyen továbbítás nem vonatkozhat a nyilvántartásban szereplő személyes adatok vagy adatkategóriák összességére, és ha a nyilvántartás célja a jogos érdekkel rendelkező személyek általi betekintés biztosítása, a nekik való továbbításra kizárólag e személyek kérelmére kerülhet sor, vagy akkor, ha ők a címzettek, teljes mértékben figyelembe véve az érintettek érdekeit és alapvető jogait.

(3) Az ismétlődőnek nem minősíthető és csupán korlátozott számú érintettre vonatkozó adattovábbítás szintén megengedhető az Adatkezelő által követett, kényszerítő erejű jogos érdekből, feltéve hogy ezen érdekekkel szemben nem élveznek elsőbbséget az érintett érdekei vagy jogai és szabadságai, és az Adatkezelő az adattovábbítás összes körülményét felmérte.

(4) Az érintett jogosult arra, hogy a rá vonatkozó, általa az Adatkezelő rendelkezésére bocsátott személyes adatokat egy másik Adatkezelőnek továbbítsa anélkül, hogy ezt akadályozná az az Adatkezelő, amelynek a személyes adatokat a rendelkezésére bocsátotta, ha:

a) az adatkezelés a GDPR 6. cikk (1) bekezdésének a) pontja vagy a GDPR 9. cikk (2) bekezdésének a) pontja szerinti hozzájáruláson, vagy a GDPR 6. cikk (1) bekezdésének b) pontja szerinti szerződésen alapul és
b) az adatkezelés automatizált módon történik.

11. Adattovábbítási nyilvántartás

27. § [Az adattovábbítási nyilvántartás]

(1) Az érintett kérelmére az Adatkezelő tájékoztatást ad az általa kezelt, illetőleg az általa megbízott feldolgozó által feldolgozott adatairól, az adatkezelés céljáról, jogalapjáról, időtartamáról, az adatfeldolgozó nevéről, címéről (székhelyéről) és az adatkezeléssel összefüggő tevékenységről. Továbbá arról, hogy kik és milyen célból kapják vagy kapták meg az adatokat. Az adattovábbításra vonatkozó nyilvántartás időtartamát az adatkezelést szabályozó jogszabály korlátozhatja. A korlátozás időtartama személyes adatok esetében öt évnél, különleges adatok esetében pedig húsz évnél rövidebb nem lehet.

(2) Az adattovábbítási nyilvántartás tartalmazza:

d) az adattovábbítás dátumát,
e) az érintett beazonosításához szükséges adatokat,
f) az adattovábbítás célját,
g) az adattovábbítás jogalapját,
h) az átadott adatok körét,
i) az adattovábbítás címzettjét.

(3) A nyilvántartás papír alapon és elektronikus úton is vezethető.

(4) Az adattovábbítási nyilvántartást jelen Szabályzat 7. számú melléklete tartalmazza.

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

28. § [Az érintett jogai]

(1) [Átlátható tájékoztatás és az érintett jogainak gyakorlására vonatkozó intézkedések]
a) Az Adatkezelőnek az érintett részére a személyes adatok kezelésére vonatkozó tájékoztatást az átláthatóság elve szerint kell nyújtania írásban (papír alapon), szóban vagy más módon (elektronikus úton).
b) Az Adatkezelőnek elő kell segítenie az érintett jogainak a gyakorlását.
c) Az Adatkezelő indokolatlan késedelem nélkül, de legkésőbb a kérelem beérkezésétől számított harminc napon belül tájékoztatja az érintettet a jogai gyakorlására irányuló kérelme nyomán hozott intézkedésekről. A határidő hosszabbítására a GDPR rendelkezései alapján van lehetőség, amelyről az érintettet tájékoztatni kell.
d) Ha az Adatkezelő nem tesz intézkedéseket az érintett kérelme alapján, indokolatlan késedelem nélkül, de legkésőbb a kérelem beérkezésétől számított harminc napon belül tájékoztatja az érintettet az intézkedés elmaradásának okairól, valamint arról, hogy az érintett panaszt nyújthat be a Hatóságnál, és élhet bírósági jogorvoslati jogával.
e) Az Adatkezelő az információkat és az érintett jogairól szóló tájékoztatást és intézkedést díjmentesen biztosítja, azonban a GDPR szerinti esetekben díjat számíthat fel.

(2) [Előzetes tájékozódáshoz való jog – ha a személyes adatokat az érintettől gyűjtik]
a) Az érintett jogosult arra, hogy az adatkezeléssel összefüggő tényekről és információkról az adatkezelés megkezdését megelőzően tájékoztatást kapjon. Ennek keretében az érintettet tájékoztatni kell:
aa) az Adatkezelő és képviselője kilétéről és elérhetőségeiről,
ab) az adatvédelmi tisztviselő vagy az adatvédelmi megbízott nevéről, elérhetőségeiről,
ac) a személyes adatok tervezett kezelésének céljáról, valamint az adatkezelés jogalapjáról,
ad) jogos érdek érvényesítésén alapuló adatkezelés esetén, az Adatkezelő vagy harmadik fél jogos érdekeiről,
ae) a személyes adatok címzettjeiről – akikkel a személyes adatot közlik -, illetve a címzettek kategóriáiról, ha van ilyen,
af) adott esetben annak tényéről, hogy az Adatkezelő harmadik országba vagy nemzetközi szervezet részére kívánja továbbítani a személyes adatokat.
b) A tisztességes és átlátható adatkezelés biztosítsa érdekében az adatkezelőnek az érintettet a következő kiegészítő információkról kell tájékoztatnia:
ba) a személyes adatok tárolásának időtartamáról, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjairól,
bb) az érintett azon jogáról, hogy kérelmezheti az Adatkezelőtől a rá vonatkozó személyes adatokhoz való hozzáférést, azok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen, valamint az érintett adathordozhatósághoz való jogáról,
bc) az érintett hozzájárulásán alapuló adatkezelés esetén arról, hogy a hozzájárulás bármely időpontban történő visszavonásához való jog, amely nem érinti a visszavonás előtt a hozzájárulás alapján végrehajtott adatkezelés jogszerűségét,
bd) a Hatósághoz címzett panasz benyújtásának jogáról,
be) arról, hogy a személyes adat szolgáltatása jogszabályon vagy szerződéses kötelezettségen alapul vagy szerződés kötésének előfeltétele-e, valamint hogy az érintett köteles-e a személyes adatokat megadni, továbbá hogy milyen lehetséges következményeikkel járhat az adatszolgáltatás elmaradása,
bf) az automatizált döntéshozatal tényéről, ideértve a profilalkotást is, valamint legalább ezekben az esetekben az alkalmazott logikáról, és arra vonatkozóan érthető információkról, hogy az ilyen adatkezelés milyen jelentőséggel, és az érintettre nézve milyen várható következményekkel bír.

c) Ha az Adatkezelő a személyes adatokon a gyűjtésük céljától eltérő célból további adatkezelést kíván végezni, a további adatkezelést megelőzően tájékoztatnia kell az érintettet erről az eltérő célról és minden releváns kiegészítő információról.

(3) [Rendelkezésre bocsátandó információk, ha a személyes adatokat nem az érintettől szerezték meg]
a) Ha az Adatkezelő a személyes adatokat nem az érintettől szerezte meg, az érintettet az Adatkezelőnek legkésőbb a személyes adatok megszerzésétől számított harminc napon belül; ha a személyes adatokat az érintettel való kapcsolattartás céljára használják, legalább az érintettel való első kapcsolatfelvétel alkalmával; vagy ha várhatóan más címzettel is közlik az adatokat, legkésőbb a személyes adatok első alkalommal való közlésekor tájékoztatnia kell a tényekről és információkról, továbbá az érintett személyes adatok kategóriáiról, valamint a személyes adatok forrásáról és adott esetben arról, hogy az adatok nyilvánosan hozzáférhető forrásokból származnak-e.
b) A további szabályokra jelen Szabályzat 28. § (2) bekezdésben (Előzetes tájékozódáshoz való jog) írtak irányadók.

(4) [Az érintett hozzáférési joga]
a) Az érintett jogosult arra, hogy az Adatkezelőtől visszajelzést kapjon arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e, és ha ilyen adatkezelés folyamatban van, jogosult arra, hogy a személyes adatokhoz és jelen Szabályzat 28. § (3) bekezdésében rögzített kapcsolódó információkhoz hozzáférést kapjon.
b) Ha személyes adatoknak harmadik országba vagy nemzetközi szervezet részére történő továbbítására kerül sor, az érintett jogosult arra, hogy tájékoztatást kapjon a továbbításra vonatkozóan a GDPR 46. cikk szerinti garanciákról.
c) Az Adatkezelőnek az adatkezelés tárgyát képező személyes adatok másolatát az érintett rendelkezésére kell bocsátania. Az érintett által kért további másolatokért az Adatkezelő az adminisztratív költségeken alapuló, ésszerű mértékű díjat számíthat fel.

(5) [A helyesbítéshez való jog]
a) Az érintett jogosult arra, hogy kérésére az Adatkezelő indokolatlan késedelem nélkül helyesbítse a rá vonatkozó pontatlan személyes adatokat.
b) Figyelembe véve az adatkezelés célját, az érintett jogosult arra, hogy kérje a hiányos személyes adatok – egyebek mellett kiegészítő nyilatkozat útján történő – kiegészítését is.

(6) [A törléshez való jog („az elfeledtetéshez való jog")]
a) Az érintett jogosult arra, hogy kérésére az Adatkezelő indokolatlan késedelem nélkül törölje a rá vonatkozó személyes adatokat, az Adatkezelő pedig köteles arra, hogy az érintettre vonatkozó személyes adatokat indokolatlan késedelem nélkül törölje ha
aa) a személyes adatokra már nincs szükség abból a célból, amelyből azokat gyűjtötték vagy más módon kezelték,
ab) az érintett visszavonja az adatkezelés alapját képező hozzájárulását, és az adatkezelésnek nincs más jogalapja,
ac) az érintett tiltakozik az adatkezelése ellen, és nincs elsőbbséget élvező jogszerű ok az adatkezelésre,
ad) a személyes adatokat jogellenesen kezelték,
ae) a személyes adatokat az Adatkezelőre alkalmazandó uniós vagy tagállami jogban előírt jogi kötelezettség teljesítéséhez törölni kell.

b) A törléshez való jog nem érvényesíthető, ha az adatkezelés szükséges
ba) a véleménynyilvánítás szabadságához és a tájékozódáshoz való jog gyakorlása céljából,
bb) az Adatkezelőre alkalmazandó uniós vagy tagállami jog szerinti kötelezettség teljesítése, illetve közérdekből vagy az Adatkezelőre ruházott közhatalmi jogosítvány gyakorlása keretében végzett feladat végrehajtása céljából,
bc) a népegészségügy területét érintő közérdek alapján,
bd) a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból, amennyiben a törléshez való jog valószínűsíthetően lehetetlenné tenné vagy komolyan veszélyeztetné ezt az adatkezelést, vagy
be) jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez,
bf) közérdekű telefonos megkeresés során az utólagos bizonyítás, valamint az adatkezeléshez való hozzájárulás, illetve tiltakozás igazolhatósága érdekében a beszélgetésről hangrögzítés készülhet.
E hangfelvétel kizárólag az érintett (hívott fél) hozzájárulása mellett készíthető, a hangfelvételt az Adatkezelő a felvételtől számított 5 évig őrzi meg, tiltakozás esetén a hangfelvétel rövid időn belül (legfeljebb 72 órán belül) törlésre kerül. A hangfelvételhez az Adatkezelő azonosítószámot rendel, ami a hívott fél telefonszáma és a beszélgetés dátuma.

(7) [Az adatkezelés korlátozásához való jog]
a) Az adatkezelés korlátozása esetén az ilyen személyes adatokat a tárolás kivételével csak az érintett hozzájárulásával, vagy jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez, vagy más természetes vagy jogi személy jogainak védelme érdekében, vagy az Unió, illetve valamely tagállam fontos közérdekéből lehet kezelni.
b) Az érintett jogosult arra, hogy kérésére az Adatkezelő korlátozza az adatkezelést, ha az alábbiak valamelyike teljesül:
ba) az érintett vitatja a személyes adatok pontosságát, ez esetben a korlátozás arra az időtartamra vonatkozik, amely lehetővé teszi, hogy az Adatkezelő ellenőrizze a személyes adatok pontosságát;
bb) az adatkezelés jogellenes, és az érintett ellenzi az adatok törlését, és ehelyett kéri azok felhasználásának korlátozását;
bc) az Adatkezelőnek már nincs szüksége a személyes adatokra adatkezelés céljából, de az érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez; vagy
bd) az érintett tiltakozott az adatkezelés ellen; ez esetben a korlátozás arra az időtartamra vonatkozik, amíg megállapításra nem kerül, hogy az Adatkezelő jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben.
c) Az adatkezelés korlátozásának feloldásáról az érintettet előzetesen tájékoztatni kell.

(8) [A személyes adatok helyesbítéséhez vagy törléséhez, illetve az adatkezelés korlátozásához kapcsolódó értesítési kötelezettség]

Az Adatkezelő minden olyan címzettet tájékoztat valamennyi helyesbítésről, törlésről vagy adatkezelés-korlátozásról, akivel, illetve amellyel a személyes adatot közölték, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel. Az érintettet kérésére az Adatkezelő tájékoztatja e címzettekről.

(9) [Az adathordozhatósághoz való jog]

a) A GDPR-ban írt feltételekkel az érintett jogosult arra, hogy a rá vonatkozó, általa az 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

aa) az adatkezelés hozzájáruláson, vagy szerződésen alapul, és
ab) az adatkezelés automatizált módon történik.
b) Az érintett kérheti a személyes adatok Adatkezelők közötti közvetlen továbbítását is.
c) Az adathordozhatósághoz való jog gyakorlása nem sértheti a GDPR 17. cikkét, azaz a törléshez való jogot. Az adathordozhatósághoz való jog nem alkalmazandó abban az esetben, ha az adatkezelés közérdekű vagy az Adatkezelőre ruházott közhatalmi jogosítványai gyakorlásának keretében végzett feladat végrehajtásához szükséges. E jog nem érintheti hátrányosan mások jogait és szabadságait.

(10) [A tiltakozáshoz való jog]

a) Az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból bármikor tiltakozzon személyes adatainak közérdeken, közfeladat végrehajtásán, vagy jogos érdeken alapuló kezelése ellen, ideértve az említett rendelkezéseken alapuló profilalkotást is. Ebben az esetben az Adatkezelő a személyes adatokat nem kezelheti tovább, kivéve, ha az adatkezelő bizonyítja, hogy az adatkezelést olyan kényszerítő erejű jogos okok indokolják, amelyek elsőbbséget élveznek az érintett érdekeivel, jogaival és szabadságaival szemben, vagy amelyek jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódnak.
b) Ha a személyes adatok kezelése közvetlen üzletszerzés érdekében történik, az érintett jogosult arra, hogy bármikor tiltakozzon a rá vonatkozó személyes adatok e célból történő kezelése ellen, ideértve a profilalkotást is, amennyiben az a közvetlen üzletszerzéshez kapcsolódik. Ha az érintett tiltakozik a személyes adatok közvetlen üzletszerzés érdekében történő kezelése ellen, akkor a személyes adatok a továbbiakban e célból nem kezelhetők.
c) Ezen jogokra legkésőbb az érintettel való első kapcsolatfelvétel során kifejezetten fel kell hívni annak figyelmét, és az erre vonatkozó tájékoztatást egyértelműen és minden más információtól elkülönítve kell megjeleníteni.
d) Az érintett a tiltakozáshoz való jogot műszaki előírásokon alapuló automatizált eszközökkel is gyakorolhatja.
e) Ha a személyes adatok kezelésére tudományos és történelmi kutatási célból vagy statisztikai célból kerül sor, az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból tiltakozhasson a rá vonatkozó személyes adatok kezelése ellen, kivéve, ha az adatkezelésre közérdekű okból végzett feladat végrehajtása érdekében van szükség.

(11) [Automatizált döntéshozatal egyedi ügyekben, beleértve a profilalkotást]
a) Az érintett jogosult arra, hogy ne terjedjen ki rá az olyan, kizárólag automatizált adatkezelésen – ideértve a profilalkotást is – alapuló döntés hatálya, amely rá nézve joghatással járna vagy őt hasonlóképpen jelentős mértékben érintené.
b) Ez a jogosultság nem alkalmazandó abban az esetben, ha a döntés:
ba) az érintett és az Adatkezelő közötti szerződés megkötése vagy teljesítése érdekében szükséges;
bb) meghozatalát az Adatkezelőre alkalmazandó olyan uniós vagy tagállami jog teszi lehetővé, amely az érintett jogainak és szabadságainak, valamint jogos érdekeinek védelmét szolgáló megfelelő intézkedéseket is megállapít, vagy
bc) az érintett kifejezett hozzájárulásán alapul.
c) Az a) és c) pontokban említett esetekben az Adatkezelő köteles megfelelő intézkedéseket tenni az érintett jogainak, szabadságainak és jogos érdekeinek védelme érdekében, ideértve az érintettnek legalább azt a jogát, hogy az Adatkezelő részéről emberi beavatkozást kérjen, álláspontját kifejezze, és a döntéssel szemben kifogást nyújtson be.

(12) [Korlátozások]
Az Adatkezelőre vagy adatfeldolgozóra alkalmazandó uniós vagy tagállami jog jogalkotási intézkedésekkel korlátozhatja jogok és kötelezettségek hatályát, ha a korlátozás tiszteletben tartja az alapvető jogok és szabadságok lényeges tartalmát.

(13) [Tájékoztatás adatvédelmi incidensről]
a) Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az Adatkezelőnek indokolatlan késedelem nélkül tájékoztatnia kell az érintettet az adatvédelmi incidensről. E tájékoztatásban világosan és közérthetően ismertetni kell az adatvédelmi incidens jellegét, és közölni kell legalább a következőket:
aa) az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit,
ab) ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket,
ac) ismertetni kell az Adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.
b) Az érintettet nem kell az tájékoztatni, ha a következő feltételek bármelyike teljesül:
ba) az Adatkezelő megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre, és ezeket az intézkedéseket az adatvédelmi incidens által érintett adatok tekintetében alkalmazták, különösen azokat az intézkedéseket – mint például a titkosítás alkalmazása –, amelyek a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik az adatokat,
bb) az Adatkezelő az adatvédelmi incidenst követően olyan további intézkedéseket tett, amelyek biztosítják, hogy az érintett jogaira és szabadságaira jelentett, magas kockázat a továbbiakban valószínűsíthetően nem valósul meg,
bc) a tájékoztatás aránytalan erőfeszítést tenne szükségessé. Ilyen esetekben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, vagy olyan hasonló intézkedést kell hozni, amely biztosítja az érintettek hasonlóan hatékony tájékoztatását.

(14) [A Hatóságnál történő panasztételhez való jog (hatósági jogorvoslathoz való jog)]
Az érintett jogosult arra, hogy panaszt tegyen egy felügyeleti hatóságnál – különösen a szokásos tartózkodási helye, a munkahelye vagy a feltételezett jogsértés helye szerinti tagállamban –, ha az érintett megítélése szerint a rá vonatkozó személyes adatok kezelése megsérti a GDPR rendelkezéseit. Az a felügyeleti hatóság, amelyhez a panaszt benyújtották, köteles tájékoztatni az ügyfelet a panasszal kapcsolatos eljárási fejleményekről és annak eredményéről, ideértve azt is, hogy az az ügyfél jogosult bírósági jogorvoslattal élni.

(15) [A Hatósággal szembeni hatékony bírósági jogorvoslathoz való jog]
a) Az egyéb közigazgatási vagy nem bírósági útra tartozó jogorvoslatok sérelme nélkül, minden természetes és jogi személy jogosult a hatékony bírósági jogorvoslatra a felügyeleti hatóság rá vonatkozó, jogilag kötelező erejű döntésével szemben.
b) Az egyéb közigazgatási vagy nem bírósági útra tartozó jogorvoslatok sérelme nélkül, minden érintett jogosult a hatékony bírósági jogorvoslatra, ha az illetékes felügyeleti hatóság nem foglalkozik a panasszal, vagy három hónapon belül nem tájékoztatja az érintettet a benyújtott panasszal kapcsolatos eljárási fejleményekről vagy annak eredményéről.
c) A Hatósággal szembeni eljárást a felügyeleti hatóság székhelye szerinti tagállam bírósága előtt kell megindítani.

d) Ha a Hatóság olyan döntése ellen indítanak eljárást, amellyel kapcsolatban az egységességi mechanizmus keretében a Testület előzőleg véleményt bocsátott ki vagy döntést hozott, a felügyeleti hatóság köteles ezt a véleményt vagy döntést a bíróságnak megküldeni.

(16) [Az Adatkezelővel szembeni hatékony bírósági jogorvoslathoz való jog]
a) A rendelkezésre álló közigazgatási vagy nem bírósági útra tartozó jogorvoslatok – különösen a felügyeleti hatóságnál történő panasztételhez való jog – sérelme nélkül, minden érintett hatékony bírósági jogorvoslatra jogosult, ha megítélése szerint a személyes adatainak, jelen Szabályzatnak nem megfelelő kezelése következtében megsértették jelen Szabályzat szerinti jogait.
b) Az Adatkezelővel szembeni eljárást az Adatkezelő tevékenységi helye szerinti tagállam bírósága előtt kell megindítani. Az ilyen eljárás megindítható az érintett szokásos tartózkodási helye szerinti tagállam bírósága előtt is, kivéve, ha az Adatkezelő vagy az adatfeldolgozó valamely tagállamnak a közhatalmi jogkörében eljáró közhatalmi szerve.

29. § [Az érintett jogainak érvényesítésével összefüggő feladatok]

(1) Az Adatkezelő elősegíti az érintett jogainak érvényesítését.
(2) Az érintett adatkezeléssel összefüggő jogait, érvényesítésük módját az Adatkezelőnek jelen Szabályzat 4. számú melléklete szerinti adatkezelési tájékoztatója tartalmazza.

13. Ellenőrzés (közreműködés a Hatósággal)

30. § [Ellenőrzés]

(1) Az Adatkezelő feladatai végrehajtása során a Hatósággal – annak megkeresése alapján – köteles együttműködni. Az Adatkezelő köteles a Hatóság utasításait betartani és tanácsait figyelembe venni.
(2) A Hatóság vizsgálatával, valamint az adatvédelmi hatósági eljárással érintett Adatkezelő szervezeti egység vezetője az adatvédelmi tisztviselő útján köteles a Hatóság részére:
a) minden szükséges tájékoztatást szóban és írásban megadni,
b) az összes olyan iratba való betekintést és másolatok készítését lehetővé tenni, amely személyes adatokkal, közérdekű adatokkal vagy közérdekből nyilvános adatokkal összefügghet,
c) biztosítani azokba a helyiségekbe való belépést, ahol adatkezelés folyik,
d) a minősített adatok megismerését elősegíteni.
(3) Az Adatkezelő tájékoztatási kötelezettségének az Infotv. 54. § (2) bekezdése alapján a Hatóság által megállapított határidőn belül köteles eleget tenni.
(4) Az Adatkezelő, illetve a tájékoztatásra felkért személy a tájékoztatást az Infotv. 54. § (3) bekezdése alapján tagadhatja meg.

14. Jogviszonnyal kapcsolatos adatkezelések

31. § [Munkaügyi, személyzeti nyilvántartás; szolgálati gépjárművezetésre vonatkozó nyilvántartás]

(1) Jogviszony alatt a közalkalmazotti jogviszonyt, a munkajogviszonyt és a közfoglalkoztatotti jogviszonyt, munkáltató alatt Adatkezelőt kell érteni.
(2) A foglalkoztatottaktól kizárólag olyan adatok kérhetők és tarthatók nyilván, valamint olyan munkaköri orvosi alkalmassági vizsgálatok végezhetők, amelyek jogviszony létesítéséhez, fenntartásához és megszüntetéséhez, illetve a szociális-jóléti juttatások biztosításához szükségesek és a foglalkoztatottak személyhez fűződő jogait nem sértik.
(3) Az Adatkezelő a foglalkoztatottak alábbi adatait kezeli:
1. név,
2. születési név,
3. születési helye, ideje,
4. anyja neve,
5. lakcíme,
6. állampolgársága,
7. adóazonosító jele,
8. TAJ száma,
9. nyugdíjas törzsszám (nyugdíjas munkavállaló esetén),

10. telefonszám,
11. e-mail cím,
12. személyazonosító okmány száma,
13. lakcímet igazoló hatósági igazolvány száma,
14. bankszámlaszáma,
15. online azonosító (ha van),
16. munkába lépésének kezdő (és befejező) időpontja,
17. munkaköre,
18. iskolai végzettségét, szakképzettségét igazoló okmány másolata a bizonyítvány számának kitakarásával,
19. fényképet,
20. önéletrajzot,
21. munkabérének összege, a bérfizetéssel, egyéb juttatásaival kapcsolatos adatokat,
22. a foglalkoztatott munkabéréből jogerős határozat vagy jogszabály, illetve írásbeli hozzájárulása alapján levonandó tartozást, illetve ennek jogosultságát,
23. a foglalkoztatott munkájának értékelését,
24. a jogviszony megszűnésének módját, indokait,
25. munkakörtől függően erkölcsi bizonyítványát,
26. a munkaköri alkalmassági vizsgálatok összegzését,
27. magán-nyugdíjpénztári és önkéntes kölcsönös biztosító pénztári tagság esetén a pénztár megnevezését, azonosító számát és a dolgozó tagsági számát,
28. külföldi foglalkoztatott esetén útlevélszámot, munkavállalási jogosultságot igazoló dokumentumának megnevezését és számát,
29. a foglalkoztatottat ért balesetek jegyzőkönyveiben rögzített adatokat,
30. a jóléti szolgáltatás vételéhez szükséges adatokat,
31. az Adatkezelőnél biztonsági és vagyonvédelmi célból alkalmazott kamera és beléptető rendszer, illetve a helymeghatározó rendszerek által rögzített adatokat.

(3) Betegségre és szakszervezeti tagságára vonatkozó adatokat a munkáltató csak a jogviszonyra irányadó meghatározott jogszabály teljesítése céljából kezel.

(4) A személyes adatok címzettjei: a munkáltatói jogkör gyakorlója, a közvetlen felettese, az Adatkezelő munkaügyi feladatokat ellátó dolgozói és adatfeldolgozói.

(5) A személyes adatok tárolásának időtartama: a jogviszony megszűnését követő 50 év.

(6) Az érintettel az adatkezelés megkezdése előtt közölni kell, hogy az adatkezelés különösen a Közalkalmazottak jogállásáról szóló törvényen, a Munka törvénykönyvén (a továbbiakban: Mt.), a vízgazdálkodásról szóló törvényen, a vízügyi igazgatási szerveknél foglalkoztatottak közalkalmazotti jogviszonyának különös szabályairól szóló Korm. rendeletben foglaltak és a munkáltató jogos érdekeinek érvényesítésén alapul.

(7) Az Adatkezelő a szolgálati gépjárművezetésre jogosult foglalkoztatottak vonatkozásában az alábbi adatokat kezeli:
1. név,
2. születési hely és idő,
3. anyja neve,
4. vezetői engedély sorszáma, érvényességi ideje.

32. § [Alkalmassági vizsgálatokkal kapcsolatos adatkezelés]

(1) A foglalkoztatottal szemben csak olyan alkalmassági vizsgálat alkalmazható, amelyet jogviszonyára vonatkozó szabály ír elő, vagy amely jogviszonyra vonatkozó szabályban meghatározott jog gyakorlása, kötelezettség teljesítése érdekében szükséges.

A vizsgálat előtt részletesen tájékoztatni kell a foglalkoztatottakat többek között arról, hogy az alkalmassági vizsgálat milyen készség, képesség felmérésére irányul, a vizsgálat milyen eszközzel, módszerrel történik.

Amennyiben jogszabály írja elő a vizsgálat elvégzését, akkor tájékoztatni kell a dolgozókat a jogszabály címéről és a pontos jogszabályhelyről is.
(2) E „Tájékoztatáshoz kapcsolódó adatkezelési tájékoztató" mintáját jelen Szabályzat 4. számú melléklete tartalmazza.
(3) A munkaalkalmasságra, felkészültségre irányuló tesztlapok a munkáltató mind a jogviszony létesítése előtt, mind pedig a jogviszony fennállása alatt intézkedhet a foglalkoztatottak általi kitöltéséről.
(4) Az egyértelműen jogviszonnyal kapcsolatos, a munkafolyamatok hatékonyabb ellátása, megszervezése érdekében csak akkor tölthető ki a foglalkoztatottak nagyobb csoportjával pszichológiai, vagy személyiségjegyek kutatására alkalmas tesztlap, ha az elemzés során felszínre került adatok nem köthetők az egyes konkrét foglalkoztatottakhoz, vagyis anonim módon történik az adatok feldolgozása.
(5) A kezelhető személyes adatok köre: a munkaköri alkalmasság ténye, és az ehhez szükséges feltételek.
(6) Az adatkezelés jogalapja: a munkáltató jogos érdeke.
(7) A személyes adatok kezelésének célja: jogviszony létesítése, fenntartása, munkakör betöltése.
(8) A személyes adatok címzettjei, illetve a címzettek kategóriái: A vizsgálat eredményt a vizsgált foglalkoztatottak, illetve a vizsgálatot végző szakember ismerhetik meg. A munkáltató kizárólag azt az információt kaphatja meg, hogy a vizsgált személy a munkára alkalmas-e vagy sem, illetve milyen feltételek biztosítandók ehhez. A vizsgálat részleteit, illetve annak teljes dokumentációját azonban a munkáltató nem ismerheti meg.
(9) A személyes adatok kezelésének időtartama: a jogviszony megszűnését követő 50 év.

33. § [Felvételre jelentkező személyek adatainak kezelése, pályázatok, önéletrajzok]
(1) A kezelhető személyes adatok köre: a természetes személy neve, születési ideje és helye, anyja neve, lakcíme, képesítési adatai, fényképe, telefonszáma, e-mail címe, a jelentkezőről készített munkáltatói feljegyzés.
(2) A személyes adatok kezelésének célja: jelentkezés, pályázat elbírálása, a kiválasztottal szerződés kötése. Az érintettet tájékoztatni kell arról, ha a munkáltató nem őt választotta az adott állásra.
(3) Az adatkezelés jogalapja: az érintett hozzájárulása.
(4) A személyes adatok címzettjei, illetve a címzettek kategóriái: az Adatkezelőnél a munkáltatói jogok gyakorlására jogosult vezető (a Főigazgatóság esetében a Főigazgató, a vízügyi igazgatóság esetében az Igazgató), munkaügyi feladatokat ellátó foglalkoztatottak.
(5) A személyes adatok tárolásának időtartama: A jelentkezés beadásától a pályázat elbírálásáig. A ki nem választott jelentkezők személyes adatait törölni kell. Törölni kell annak adatait is, aki jelentkezését, pályázatát visszavonta. A személyes adatok megőrzése a pályázó hozzájárulásával, a pályázat elbírálásától számított hat hónapig lehetséges.
(6) A munkáltató csak az érintett kifejezett, egyértelmű és önkéntes hozzájárulása alapján őrizheti meg a pályázatokat, feltéve, ha azok megőrzésére a jogszabályokkal összhangban álló adatkezelési célja elérése érdekében szükség van. E hozzájárulást a felvételi eljárás lezárását követően kell kérni a jelentkezőktől.

34. § [E-mail fiók használatának ellenőrzésével kapcsolatos adatkezelés]
(1) Ha az Adatkezelő e-mail fiókot bocsát a foglalkoztatott rendelkezésére – ezen e-mail címet és fiókot a foglalkoztatott kizárólag munkaköri feladatai céljára használhatja, annak érdekében, hogy a foglalkoztatottak ezen keresztül tartsák egymással a kapcsolatot, vagy a munkáltató képviseletében levelezzenek a felügyeleti- és társ szervekkel, az ügyfelekkel, más személyekkel, szervezetekkel.
(2) A foglalkoztatott az e-mail fiókot személyes célra nem használhatja, a fiókban személyes leveleket nem tárolhat.

(3) Az Adatkezelő elektronikus címjegyzékének külső személy vagy szervezet részére történő továbbítása tilos.
(4) Tilos külső személy vagy szervezet részére az elektronikus levelek automatikus továbbítása.
(5) A munkáltató jogosult az e-mail fiók teljes tartalmát és használatát rendszeresen, előzetes értesítést követően – 3 havonta – ellenőrizni, ennek során az adatkezelés jogalapja a munkáltató jogos érdeke. Az ellenőrzés célja az e-mail fiók használatára vonatkozó munkáltatói rendelkezés betartásának ellenőrzése, továbbá a foglalkoztatottak kötelezettségeinek (Mt. 8. §, 52. §) ellenőrzése.
(6) Az ellenőrzésre és adatkezelésre a Főigazgatóság esetében a Főigazgató, a vízügyi igazgatóság esetében az Igazgató, illetve az Informatikai Főosztály vezetője jogosult.
(7) Amennyiben az ellenőrzés körülményei nem zárják ki ennek lehetőségét, biztosítani kell, hogy a foglalkoztatott jelen lehessen az ellenőrzés során.
(8) Az ellenőrzés előtt jelen Szabályzat 9. számú melléklete szerint tájékoztatni kell a foglalkoztatottat arról, hogy milyen munkáltatói érdek miatt kerül sor az ellenőrzésre, munkáltató részéről ki végezheti az ellenőrzést, – milyen szabályok szerint kerülhet sor ellenőrzésre (fokozatosság elvének betartása) és mi az eljárás menete, – milyen jogai és jogorvoslati lehetőségei vannak az e-mail fiók ellenőrzésével együtt járó adatkezeléssel kapcsolatban.
(9) Az ellenőrzés során a fokozatosság elvét kell alkalmazni, így elsődlegesen az e-mail címéből és tárgyából kell megállapítani, hogy az a foglalkoztatott munkaköri feladatával kapcsolatos, és nem személyes célú. Nem személyes célú e-mailek tartalmát a munkáltató korlátozás nélkül vizsgálhatja.
(10) Ha jelen Szabályzat rendelkezéseivel ellentétben az állapítható meg, hogy a foglalkoztatott az e-mail fiókot személyes célra használta, fel kell szólítani a foglalkoztatottat, hogy a személyes adatokat haladéktalanul törölje. A foglalkoztatott távolléte, vagy együttműködésének hiánya esetén a személyes adatokat az ellenőrzéskor a munkáltató törli. Az e-mail fiók jelen szabályzattal ellentétes használata miatt a munkáltató a foglalkoztatottal szemben munkajogi jogkövetkezményeket alkalmazhat.
(11) A foglalkoztatott az e-mail fiók ellenőrzésével együtt járó adatkezeléssel kapcsolatban jelen Szabályzatnak az érintett jogairól szóló fejezetében rögzített jogokkal élhet.

35. § [Számítógép, laptop, tablet ellenőrzésével kapcsolatos adatkezelés]

(1) Az Adatkezelő által a foglalkoztatott részére munkavégzés céljára rendelkezésre bocsátott számítógépet, laptopot, tabletet a foglalkoztatott kizárólag munkaköri feladata ellátására használhatja, ezek magáncélú használatát az Adatkezelő megtiltja, ezen eszközökön a foglalkoztatott semmilyen személyes adatot, levelezést nem kezelhet, és nem tárolhat.
(2) A munkáltató ezen eszközökön tárolt adatokat ellenőrizheti.
(3) Ezen eszközök munkáltató általi ellenőrzésére és jogkövetkezményire egyebekben jelen Szabályzat 34. §-ában rögzített rendelkezések irányadók.

36. § [A munkahelyi internethasználat ellenőrzésével kapcsolatos adatkezelés]
(1) A foglalkoztatott csak a munkaköri feladatával kapcsolatos honlapokat tekintheti meg, a személyes célú munkahelyi internethasználatot a munkáltató megtiltja. Főszabály szerint tilos a foglalkoztatott által közösségi oldalak (social media) látogatása, azonban meghatározott munkakörök ellátása esetében a munkáltató jogosult engedélyezni ezen oldalak használatát a foglalkoztatott részére.
(2) Hivatali e-mail címmel a hivatali tevékenységhez nem köthető on-line szolgáltatásra regisztrálni tilos. A munkaköri feladatként az Adatkezelő nevében elvégzett internetes regisztrációk jogosultja az Adatkezelő, a regisztráció során az Adatkezelőre utaló azonosítót, jelszót kell alkalmazni, amely azonban nem egyezhet meg a regisztráló foglalkoztatott hivatali jelszavával. Amennyiben a személyes adatok megadása is szükséges a regisztrációhoz, a jogviszony megszűnésekor azok törlését köteles kezdeményezni az Adatkezelő.

(3) A foglalkoztatott munkahelyi internethasználatát a munkáltató előzetes értesítést követően ellenőrizheti, amelyre és jogkövetkezményeire jelen Szabályzat 34. §-ában rögzített rendelkezések irányadók.

37. § [Céges mobiltelefon használatának ellenőrzésével kapcsolatos adatkezelés]
(1) A munkáltató céges valamennyi kimenő hívás hívószámát és adatait, továbbá a mobiltelefonon tárolt adatokat ellenőrizheti. A munkáltató szabályzattal (belső szabályozási norma) rendelkezik a céges telefonok használatáról.
(2) Egyebekben az ellenőrzésre és jogkövetkezményire jelen Szabályzat 34. §-ában rögzített rendelkezések irányadók.

38. § [Munkahelyi be- és kiléptetéssel kapcsolatos adatkezelés]
(1) A kezelhető személyes adatok köre: a természetes személy neve, lakcíme, személygépjármű rendszáma, belépés és kilépés ideje.
(2) Az adatkezelés jogalapja: a munkáltató jogos érdekeinek érvényesítése.
(3) A személyes adatok kezelésének célja: vagyonvédelem, szerződés teljesítése, dolgozói kötelezettségek teljesítésének ellenőrzése.
(4) A személyes adatok címzettjei: az Adatkezelőnél a munkáltatói jogok gyakorlására jogosult vezető (a Főigazgatóság esetében a Főigazgató, a vízügyi igazgatóságok esetében az Igazgató), illetve az Informatikai Főosztály vezetője.
(5) A személyes adatok kezelésének időtartama:
a) rendszeres belépés esetén a jogosultság megszűnéséig, legkésőbb az adat keletkezésétől számított 6 hónap elteltéig,
b) alkalmi belépés esetén a távozástól számított 24 óráig.

39. § [Munkahelyi kamerás megfigyeléssel kapcsolatos adatkezelés]
(1) Az Adatkezelő a székhelyén és telephelyein az emberi élet, testi épség, személyi szabadság, az üzleti titok védelme és a vagyonvédelem céljából elektronikus megfigyelőrendszert alkalmaz, amely közvetlen megfigyelést (képrögzítést) és tárolást is lehetővé tesz, ez alapján személyes adatnak tekinthető az érintett magatartása is, amit a kamera rögzít.
(2) Ezen adatkezelés jogalapja a munkáltató jogos érdekeinek érvényesítése, és az érintett hozzájárulása.
(3) Az elektronikus megfigyelőrendszer adott területen történő alkalmazásának tényéről jól látható helyen, jól olvashatóan, a területen megjelenni kívánó harmadik személyek tájékozódását elősegítő módon figyelemfelhívó jelzést, tájékoztatást kell elhelyezni. A tájékoztatást minden egyes kamera vonatkozásában meg kell adni.
Ez a tájékoztatás tartalmazza az elektronikai vagyonvédelmi rendszer által folytatott megfigyelés tényéről, valamint a rendszer által rögzített, személyes adatokat tartalmazó képfelvétel készítésének, tárolásának céljáról, az adatkezelés jogalapjáról, a felvétel tárolásának helyéről, a tárolás időtartamáról, a rendszert alkalmazó személyéről, az adatok megismerésére jogosult személyek köréről, a felvétel tárolásával kapcsolatos adatbiztonsági intézkedésekről, továbbá az érintettek jogaira és érvényesítésük rendjére vonatkozó tájékoztatást is. A tájékoztatás mintáját jelen Szabályzat 10. számú melléklete rögzíti. A tájékoztató elhelyezésére a belépési helyeken kerül sor.
(4) A megfigyelt területre belépő harmadik személyekről (ügyfelek, látogatók, vendégek) képfelvétel a hozzájárulásukkal készíthető és kezelhető. A hozzájárulás ráutaló magatartással is megadható. Ráutaló magatartás különösen, ha az ott tartózkodó természetes személy a megfigyelt területre az oda kihelyezett elektronikus megfigyelő-rendszer alkalmazásáról tájékoztató jelzés, ismertetés ellenére a területre bemegy.

(5) A rögzített felvételeket felhasználás hiányában főszabály szerint legfeljebb három munkanapig őrizhetők meg. Felhasználásnak az minősül, ha a rögzített képfelvételt, valamint más személyes adatot bírósági vagy más hatósági eljárásban bizonyítékként kívánják felhasználni. Az Adatkezelő 72 órát meghaladó adatkezelésre jogosult, amennyiben jogos érdeke fűződik az adatok hosszabb idejű tárolásához.
(6) Adatbiztonsági intézkedések:
a) A képfelvételek megtekintésére és visszanézésére szolgáló monitor úgy kell elhelyezni, hogy a képfelvételek sugárzása alatt azokat a jogosultsági körön kívül más személy ne láthassa.
b) A megfigyelés és a tárolt képfelvételek visszanézése kizárólag a jogsértő cselekmények kiszűrése, az azok megszüntetéséhez szükséges intézkedések kezdeményezése céljából végezhető.
c) A kamerák által sugárzott képekről a központi felvevő egységen kívül más eszközzel felvételt készíteni nem lehet.
d) A felvétel hordozó eszközeit elzárt helyen kell tárolni.
e) A tárolt képfelvételekhez hozzáférés csak biztonságos módon, és akként történhet, hogy az Adatkezelő személye azonosítható legyen.
f) A tárolt képfelvételek visszanézését és a képfelvételekről készített mentést dokumentálni kell.
g) A jogosultság indokának megszűnése esetén a tárolt képfelvételekhez a hozzáférést haladéktalanul meg kell szüntetni.
h) A rögzítő készülékben elkülönített merevlemezről fut az operációs rendszer és a rögzítésre került felvételek. A felvételekről külön biztonsági másolat nem készül.
i) Jogsértő cselekmény észlelését követően a cselekményről készült felvétel tárolása és a szükséges hatósági eljárás kezdeményezése felől haladéktalanul intézkedni kell, és egyben tájékoztatni kell az illetékes hatóságot, hogy a cselekményről képfelvétel készült.
(7) Az, akinek jogát vagy jogos érdekét képfelvétel adatának rögzítése érinti, a képfelvétel rögzítésétől számított három munkanapon belül jogának vagy jogos érdekének igazolásával kérheti a szervezet vezetőjétől, hogy az adatot annak kezelője ne semmisítse meg, illetve ne törölje.
(8) Nem lehet elektronikus megfigyelőrendszert alkalmazni olyan helyiségben, amelyben a megfigyelés az emberi méltóságot sértheti, így különösen az öltözőkben, zuhanyzókban, az illemhelyiségekben, továbbá az olyan helyiségben sem, amely a dolgozók munkaközi szüneteinek eltöltése céljából lett kijelölve.
(9) Ha a munkavégzési hely területén jogszerűen senki sem tartózkodhat - így különösen munkaidőn kívül vagy a munkaszüneti napokon - akkor a munkahely teljes területe (így például az öltözők, illemhelyek, munkaközi szünetre kijelölt helyiségek) megfigyelhető.
(10) Az elektronikus megfigyelőrendszerrel rögzített adatok megtekintésére a törvényben erre feljogosítottakon kívül a jogsértések feltárása és a rendszer működésének ellenőrzés céljából a megfigyelt terület munkáltatói jogköröket gyakorló vezetője is jogosult.

15. A szerződéshez kapcsolódó adatkezelések

40. § [Szerződéses partnerek adatainak kezelése]

(1) Az Adatkezelő szerződés teljesítése jogcímén a szerződés megkötése, teljesítése, megszűnése céljából kezeli a vele vevőként, szállítóként, vállalkozóként szerződött természetes személy nevét, születési nevét, születési idejét, anyja nevét, lakcímét, adóazonosító jelét, adószámát, vállalkozói, őstermelői igazolvány számát, személyi igazolvány számát, lakcímét, székhely, telephely címét, telefonszámát, e-mail címét, honlap-címét, bankszámlaszámát, vevőszámát (ügyfélszámát, rendelésszámát), online azonosítóját. Ezen adatkezelés jogszerűnek minősül akkor is, ha az adatkezelés a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges. A személyes adatok címzettjei: az Adatkezelő szerződésekkel kapcsolatos feladatokat ellátó foglalkoztatottjai.

(2) A személyes adatok tárolásának időtartama: a szerződés megszűnését követő 15 év.
(3) Az érintett természetes személlyel az adatkezelés megkezdése előtt közölni kell, hogy az adatkezelés a szerződés teljesítése jogcímén alapul, az a tájékoztatás történhet a szerződésben is. Az érintettet személyes adatai adatfeldolgozó részére történő átadásáról tájékoztatni kell.

41. § [Jogi személy ügyfelek, vevők, szállítók természetes személy képviselőinek elérhetőségi adatai]
(1) A kezelhető személyes adatok köre: a természetes személy neve, címe, telefonszáma, e-mail címe, online azonosítója.
(2) A személyes adatok kezelésének célja: az Adatkezelő jogi személy partnerével kötött szerződés teljesítése, üzleti kapcsolattartás, jogalapja: az érintett hozzájárulása.
(3) A személyes adatok címzettjei, illetve a címzettek köre: az Adatkezelő PR-ral kapcsolatos feladatokat ellátó foglalkoztatottjai.
(4) A személyes adatok tárolásának időtartama: az üzleti kapcsolat, illetve az érintett képviselői minőségének fennállását követő 15 évig.
(5) Az adatfelvételi lap mintáját jelen Szabályzat 6. számú melléklete tartalmazza. Ezen nyilatkozatot az ügyféllel, vevővel, szállítóval kapcsolatban álló foglalkoztatottnak ismertetnie kell az érintett személlyel és a nyilatkozat aláírásával kérnie kell hozzájárulását személyes adatai kezeléséhez. A nyilatkozatot az adatkezelés időtartamáig meg kell őrizni.

42. § [Látogatói adatkezelés az Adatkezelő honlapján - Tájékoztatás sütik (cookie) alkalmazásáról]

(1) A süti (angolul cookie) egy olyan adat, amit a meglátogatott weboldal küld a látogató böngészőjének (változónév-érték formában), hogy az eltárolja és később ugyanaz a weboldal be is tudja tölteni a tartalmát.
(2) Egy felhasználónak az elektronikus hírközlő végberendezésén csak az érintett felhasználó világos és teljes körű – az adatkezelés céljára is kiterjedő – tájékoztatását követő hozzájárulása alapján lehet adatot tárolni, vagy az ott tárolt adathoz hozzáférni. Ez alapján az Adatkezelő honlapján az első látogatáskor egy rövid összefoglalót kell adni a látogató számára a sütik alkalmazásáról, és egy linken keresztül utalni kell a teljes körű tájékoztató elérhetőségére. E tájékoztatóval az Adatkezelő biztosítja, hogy a látogató a honlap információs társadalommal összefüggő szolgáltatásainak igénybevétele előtt és az igénybevétel során bármikor megismerhesse, hogy az Adatkezelő mely adatkezelési célokból mely adatfajtákat kezel, ideértve az igénybe vevővel közvetlenül kapcsolatba nem hozható adatok kezelését is.
(3) A szolgáltató a szolgáltatás nyújtása céljából kezelheti azon személyes adatokat, amelyek a szolgáltatás nyújtásához technikailag elengedhetetlenül szükségesek. A szolgáltatónak az egyéb feltételek azonossága esetén úgy kell megválasztania és minden esetben oly módon kell üzemeltetnie az információs társadalommal összefüggő szolgáltatás nyújtása során alkalmazott eszközöket, hogy személyes adatok kezelésére csak akkor kerüljön sor, ha ez a szolgáltatás nyújtásához és az e törvényben meghatározott egyéb célok teljesüléséhez feltétlenül szükséges, azonban ebben az esetben is csak a szükséges mértékben és ideig.

16. Jogi kötelezettség teljesítésén alapuló adatkezelések

43. § [Adatkezelés adó- és számviteli kötelezettségek teljesítése céljából]
(1) Az Adatkezelő jogi kötelezettség teljesítése jogcímén, törvényben előírt adó és számviteli kötelezettségek teljesítése (könyvelés, adózás) céljából kezeli a vevőként, szállítóként vele üzleti kapcsolatba lépő természetes személyek törvényben meghatározott adatait.

(2) A kezelt adatok az általános forgalmi adóról szóló 2017. évi CXXVII. törvény 169. §-a és 202. §-a alapján különösen: adószám, név, cím, adózási státusz, a számvitelről szóló 2000. évi C. törvény 167. §-a alapján: név, cím, a gazdasági műveletet elrendelő személy vagy szervezet megjelölése, az utalványozó és a rendelkezés végrehajtását igazoló személy, valamint a szervezettől függően az ellenőr aláírása; a készletmozgások bizonylatain és a pénzkezelési bizonylatokon az átvevő, az ellennyugtákon a befizető aláírása, a személyi jövedelemadóról szóló 1995. évi CXVII. törvény alapján: vállalkozói igazolvány száma, őstermelői igazolvány száma, adóazonosító jel.
(3) A személyes adatok tárolásának időtartama a jogalapot adó jogviszony megszűnését követő 8 év.
(4) A személyes adatok címzettjei: az Adatkezelő adózási, könyvviteli, bérszámfejtési, társadalombiztosítási feladatait ellátó foglalkoztatottjai és adatfeldolgozói (Magyar Államkincstár).

44. § [Kifizetői adatkezelés]
(1) Az Adatkezelő jogi kötelezettség teljesítése jogcímén, törvényben előírt adó- és járulékkötelezettségek teljesítése (adó-, adóelőleg, járulékok megállapítása, bérszámfejtés, társadalombiztosítási, nyugdíj ügyintézés) céljából kezeli azon érintettek – foglalkoztatottak, családtagjaik, egyéb juttatásban részesülők – adótörvényekben előírt személyes adatait, akikkel kifizetői kapcsolatban áll. A kezelt adatok körét az adózás rendjéről szóló 2017. évi CL. törvény 50. §-a határozza meg, különösen: a természetes személy természetes személyazonosító adatai (ideértve az előző nevet és a titulust is), neme, állampolgársága, a természetes személy adóazonosító jele, társadalombiztosítási azonosító jele (TAJ szám). Amennyiben az adótörvények ehhez jogkövetkezményt fűznek, az Adatkezelő kezelheti a foglalkoztatottak egészségügyi és szakszervezeti tagságra vonatkozó adatait adó- és járulékkötelezettségek teljesítés (bérszámfejtés, társadalombiztosítási ügyintézés) céljából.
(2) A személyes adatok tárolásának időtartama a jogalapot adó jogviszony megszűnését követő 30 év.
(3) A személyes adatok címzettjei: az Adatkezelő adózási, bérszámfejtési, társadalombiztosítási (kifizetői) feladatait ellátó foglalkoztatottjai és adatfeldolgozói (Magyar Államkincstár).

45. § [A Levéltári törvény szerint maradandó értékű iratokra vonatkozó adatkezelés]
(1) Az Adatkezelő jogi kötelezettsége teljesítése jogcímén kezeli a köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről szóló 1995. évi LXVI. törvény (Levéltári törvény) szerint maradandó értékűnek minősülő iratait abból a célból, hogy az Adatkezelő irattári anyagának maradandó értékű része épségben és használható állapotban a jövő nemzedékei számára is fennmaradjon.
(2) Az adattárolás ideje: a közlevéltár részére történő átadásig 15 év.
(3) A személyes adatok címzettjei: az Adatkezelő iratkezelést, irattárazást végző foglalkoztatottak, a közlevéltár munkatársa.

17. Adatbiztonsági intézkedések

46. § [Adatbiztonsági intézkedések]
(1) Az Adatkezelő valamennyi célú és jogalapú adatkezelése vonatkozásában a személyes adatok biztonsága érdekében köteles megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek a GDPR és az Infotv., érvényre juttatásához szükségesek.
(2) Az Adatkezelő az adatokat megfelelő intézkedésekkel védi a véletlen vagy jogellenes megsemmisítés, elvesztés, megváltoztatás, sérülés, jogosulatlan nyilvánosságra hozatal vagy az azokhoz való jogosulatlan hozzáférés 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 az Igazgatóság eszközein fájl letöltő-, 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) Biztosítani kell az adatok és az azokat hordozó eszközök, iratok megfelelő fizikai védelmét.

18. Az Adatkezelő által kezelt közérdekű és közérdekből nyilvános adatok megismerése

47. § [A közérdekű adatok és a közérdekből nyilvános adatok megismerése]

Az Adatkezelő által kezelt közérdekű és közérdekből nyilvános adatok megismerésével összefüggő szabályokat a közérdekű adatok közzétételéről és a megismerésükre vonatkozó igények teljesítésének rendjéről szóló főigazgatói utasítás tartalmazza.

19. Oktatás, vizsgáztatás

48. § [Oktatás, vizsgáztatás]

Az Adatkezelő a közalkalmazotti továbbképzés keretében a GDPR-ban és az Infotv.-ben meghatározott főbb szabályok ismertetése céljából adatvédelmi oktatást szervez. Az Adatkezelő fenntartja a jogot, hogy a foglalkoztatottjai oktatására harmadik féllel szerződjön. Az adatvédelmi oktatás módját, tematikáját, feltételeit, a vizsgáztatás rendjét, az oktatási program pontértékét a főigazgató határozza meg.

III. ZÁRÓ RENDELKEZÉSEK

49. § Jelen Szabályzat 2019. június 17. napján lép hatályba, ezzel egyidejűleg hatályát veszíti a 66/2013. (OVF) számú főigazgatói utasítás I-II., valamint IV. fejezete, valamint annak mellékletei.
50. § Jelen Szabályzat felülvizsgálatáért és aktualizálásáért a Főigazgatói Hivatal vezetője felel.
51. § Jelen Szabályzatban foglaltakat a Főigazgatóság és a vízügyi igazgatóságok valamennyi foglalkoztatottja köteles megismerni és betartani.

52. § Jelen Szabályzatban foglaltak betartásáért a Főigazgató és az igazgatók, valamint valamennyi szervezeti egység vezetője az általa irányított szervezeti egység vonatkozásában felelősséggel tartozik.
53. § A vízügyi igazgatóságok jelen Szabályzat hatályba lépését követő 60 napon belül kötelesek felülvizsgálni és szükség szerint megalkotni az Igazgatóságukra vonatkozó részletszabályokat, amelyek nem lehetnek ellentétesek jelen Szabályzat rendelkezéseivel; valamint e tárgykörben kiadott szabályzatok hatályon kívül helyezéséről haladéktalanul intézkedni kötelesek.
54. § Jelen Szabályzat mellékleteit az Adatkezelő köteles közzétenni honlapján, megfelelő fejléc alkalmazásával, letölthető formátumban.

Budapest, 2019. június „ „

.....
Láng István
főigazgató

1. számú melléklet

ADATKEZELÉSI HOZZÁJÁRULÁS

személyes adatok kezeléséhez

Alulírott ……. (név),

lakcím: ……..

szül. hely és idő: ……..

anyja neve: ……

a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) szóló, az Európai Parlament és a Tanács (EU) 2016/679 rendelete (GDPR) 6. cikk (1) bekezdés a) pontja, valamint az információs önrendelkezési jogról és információszabadságról szóló 2011. évi CXII. törvény 5. § (1) bekezdés a) pontja alapján hozzájárulok ahhoz, hogy az Országos Vízügyi Főigazgatóság, mint Adatkezelő az általam az ügyintézés során megadott személyes adatokat
a(z)……..……..
……céljából kezelje.

Az általam megadott személyes adatok köre, fajtája (a megfelelő aláhúzandó):

név, születési név, leánykori név, születési hely és idő, anyja neve, állampolgárság, személyazonosító igazolvány szám, személyi azonosító, adóazonosító jel, társadalombiztosítási azonosító jel, telefonszám, e-mail-cím, lakcím, tartózkodási hely, számlázási cím, bankszámlaszám,

egyéb megadott személyes adat köre, fajtája:

……
……

Kijelentem, hogy az általam szolgáltatott személyes adatokat önkéntesen és megfelelő tájékoztatást követően adtam meg, azok valóságtartalmáért felelősséget vállalok.

Kelt: ……..……., …… év ……. hó …. nap

……..……

név, aláírás

2. sz. melléklet

…… adatkezelés

adatvédelmi hatásvizsgálata

A tervezett adatkezelési műveletek módszeres leírása	
Az adatkezelés céljainak ismertetése	
Adatkezelő által érvényesíteni kívánt jogos érdek	
Az adatkezelés szükségességi és arányossági vizsgálata és eredménye	
Az érintett jogait és szabadságait érintő kockázatok vizsgálata és eredménye	
A kockázatok kezelését célzó intézkedések bemutatása	

3. számú melléklet

Adatvédelmi incidens nyilvántartás

Adatvédelmi tisztviselő neve, elérhetőségei	
Incidenssel érintett személyes adatok kategóriái	
Érintettek kategóriái és hozzávetőleges számuk	
Adatvédelmi incidens bekövetkeztének ideje	
Adatvédelmi incidens körülményei, hatása	
Az adatkezelési incidens orvoslására tett vagy tervezett intézkedések	
Az adatkezelést előíró jogszabályban meghatározott egyéb adatok	

4. sz. melléklet

Az Országos Vízügyi Főigazgatóság / ……. Vízügyi Igazgatóság adatkezelési tájékoztatója

1. Adatkezelő, adatvédelmi tisztviselő és adatfeldolgozó megnevezése:

Adatkezelő: Országos Vízügyi Igazgatóság (a továbbiakban: OVF) / ……. Vízügyi Igazgatóság (a továbbiakban: Igazgatóság)

Székhely: 1012 Budapest, Márvány utca 1/d. / ……

E-mail: ovf@ovf.hu / ……

Telefon: 1/225-4400 / ……

Adatvédelmi tisztviselő neve: ……..

Adatvédelmi tisztviselő e-mail címe: ……..

Adatvédelmi tisztviselő telefonszáma: ……..

Papír alapú postai küldemények adatfeldolgozója: Magyar Posta Zrt.

Székhely: 1138 Budapest, Dunavirág utca 2-6. Postacím: 1540 Budapest

E-mail: kozadat@posta.hu

Telefon: 1/767-8282

Fax: 46/620-136

Elektronikus küldemények adatfeldolgozója: Nemzeti Infokommunikációs Szolgáltató Zrt.

Székhely: 1081 Budapest, Csokonai utca 3. Postacím: 1389 Budapest, Pf. 133.

E-mail: info@nisz.hu

Telefon: 1/459-4200

Fax: 1/303-1000

2. Az adatkezelés alapjául szolgáló jogszabályok:

a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) szóló, az Európai Parlament és a Tanács (EU) 2016/679 rendelete (GDPR); a Polgári Törvénykönyvről szóló 2013. évi V. törvény (Ptk.); az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Infotv.); a köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről szóló 1995. évi LXVI. törvény, a számvitelről szóló 2000. évi C. törvény; az általános forgalmi adóról szóló 2007. évi CXXVII. törvény; a közfeladatot ellátó szervek iratkezelésének általános követelményeiről szóló 335/2005. (XII. 29.) Korm. rendelet.

3. Az érintett jogai:

- kérelmezheti a személyes adataihoz való hozzáférést;

- kérelmezheti a személyes adatainak helyesbítését, kiegészítését, kezelésének korlátozását vagy törlését;

- az Adatkezelőnél kezdeményezheti a megadott személyes adatainak tagolt, naprakész és gépileg olvasható formátumban való kiadását (adathordozhatósághoz való jog) vagy továbbítását egy másik személy részére;

- tiltakozhat a személyes adatai kezelése ellen;

- az adatkezelési hozzájárulását bármely időpontban visszavonhatja.

Az érintett jogainak érvényesítését az Adatkezelő bármely elérhetőségén kezdeményezheti. Az ügyintézési határidő a kérelem beérkezésétől számított 25 nap, tiltakozási jog gyakorlása esetén 15 nap. Az érintett továbbá: - panaszt nyújthat be a felügyeleti hatósághoz vélelmezett jogsérelem esetén (Nemzeti Adatvédelmi és Információszabadság Hatóság, webcím: https://naih.hu, telefonszám: +36 (1) 391-1400, postacím: 1530 Budapest, Pf.: 5., e-mail: ugyfelszolgalat@naih.hu)

- bírósághoz fordulhat vélelmezett jogsérelem esetén.

Felhívjuk az OVF / Igazgatóság részére adatot közlők figyelmét, hogy amennyiben nem a saját személyes adataikat adják meg, az adatközlő kötelessége az érintett hozzájárulásának beszerzése.

4. Az érintett tájékoztatása az adatvédelmi incidensről

Az Adatkezelő indokolatlan késedelem nélkül tájékoztatja az érintettet az őt érintő adatvédelmi incidensről.

5. Az adatkezelés céljai:

a) munkavégzésre irányuló jogviszony létesítése, fenntartása, megszüntetése,

b) szerződéses jogviszony létesítése, fenntartása, módosítása, teljesítése, megszüntetése,

(A szerződések teljesítéshez szükséges személyes adatok közlése (pl. szerződéskötő fél személyes adatainak szolgáltatása) a szerződés kötésének előfeltétele. Az adatszolgáltatás elmaradása esetén az OVF-nek / Igazgatóságnak nem áll módjában szerződést kötni az érintettel.)

c) vízgazdálkodási feladatok teljesítése,

d) számviteli és gazdálkodási feladatok teljesítése,

e) egyéb igazgatási feladatok teljesítése.

6. Kezelt adatok köre: név, születési név, leánykori név, születési hely és idő, anyja neve, állampolgárság, személyazonosító igazolvány szám, személyi azonosító, adóazonosító jel, társadalombiztosítási azonosító jel, telefonszám, e-mail-cím, lakcím, tartózkodási hely, számlázási cím, bankszámlaszám, beosztás, munkakör, törzsszám, családi állapot, eltartottak neve, gyermekeinek születési ideje, legmagasabb iskolai végzettség, szakképzettség, tudományos fokozat, idegennyelv-ismeret, címek, kitüntetések, személyi juttatások, nyugdíjpénztári tagság, önkéntes nyugdíjpénztári tagság, fénykép, mozgókép és a természetes személyre vonatkozó egyéb adatok.

7. Az adatkezelés jogalapja: érintett hozzájárulása, szerződés és jogi kötelezettség teljesítése. A GDPR 6. cikk (1) bekezdése alapján:

a) az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez;

b) az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél, vagy az a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges;

c) az adatkezelés az Adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges;

d) az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges;

e) az adatkezelés közérdekű feladat végrehajtásához szükséges;

f) az adatkezelés az Adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges.

8. Az adatkezelés időtartama: ügyintézés ideje, közfeladat ellátásának ideje, cél megvalósulása, irattári őrzési idő letelte, szerződéses jogviszony tartama, jogvita időtartama, jogszabályban meghatározott őrzési idő letelte.

9. Címzettje adott esetben: különösen a Belügyminisztérium, Magyar Államkincstár, Kormányhivatal, Magyar Nemzeti Vagyonkezelő Zrt., Nemzeti Földalapkezelő Szervezet, Nemzeti Adó- és Vámhivatal, könyvvizsgáló, Állami Számvevőszék, Kormányzati Ellenőrzési Hivatal, közjegyző, oktatási és képzőhelyek, bíróság, egyéb hatóságok.

A személyes adatok kezelésének jogszerűnek és tisztességesnek kell lennie. A természetes személyek számára átláthatónak kell lennie, hogy a rájuk vonatkozó személyes adataikat hogyan gyűjtik, használják fel, azokba hogy tekintenek bele vagy milyen egyéb módon kezelik, valamint azzal összefüggésben, hogy a személyes adatokat milyen mértékben kezelik vagy fogják kezelni. Az átláthatóság elve megköveteli, hogy a személyes adatok kezelésével összefüggő tájékoztatás, illetve kommunikáció könnyen hozzáférhető és közérthető legyen, valamint hogy azt világosan és egyszerű nyelvezettel fogalmazzák meg. Ez az elv vonatkozik különösen az érintetteknek az Adatkezelő kilétéről és az adatkezelés céljáról való tájékoztatására, valamint az azt célzó további tájékoztatásra, hogy biztosított legyen az érintett személyes adatainak tisztességes és átlátható kezelése, továbbá arra a tájékoztatásra, hogy az érintetteknek jogukban áll megerősítést és tájékoztatást kapni a róluk kezelt adatokról. A természetes személyt a személyes adatok kezelésével összefüggő kockázatokról, szabályokról, garanciákról és jogokról tájékoztatni kell, valamint arról, hogy hogyan gyakorolhatja az adatkezelés kapcsán megillető jogokat. A személyes adatkezelés konkrét céljainak mindenekelőtt explicit módon megfogalmazottaknak és jogszerűeknek, továbbá már a személyes adatok gyűjtésének időpontjában meghatározottaknak kell lenniük.

5. számú melléklet

Adattörlési nyilvántartás

Sorszám	Kérelem időpontja	Kérelmező neve	Kérelem tartalma	Megtett intézkedés
1.				
2.				
3.				
4.				
5.				

6. számú melléklet

…… (tevékenység) adatkezelési nyilvántartása

Adatkezelő neve, elérhetőségei	Országos Vízügyi Főigazgatóság székhely: 1012 Budapest, Márvány u. 1/d. telefon: 1/225-4400 e-mail: ovf@ovf.hu …….. Vízügyi Igazgatóság
Adatkezelő képviselőjének neve, beosztása	Láng István főigazgató ……. igazgató
Adatvédelmi tisztviselő neve, elérhetőségei	
Kitöltés dátuma	
Adatkezelés célja	
Adatkezelés jogalapja	
Érintettek kategóriái	
Személyes adatok kategóriái	
Címzettek kategóriái	
Adattovábbítás harmadik országba vagy nemzetközi szervezet részére	

Az adatkategóriák törlésére előirányzott határidők, a törlés időpontja	
Adatkezelés biztonságának leírása	
Szervezeten belül a személyes adatokhoz való hozzáférés ismertetése	
Személyes adatok tárolásának helye	
Személyes adatok tárolásának formája	
Adatfeldolgozó neve, képviselője és elérhetősége	
Adatkezelésre vonatkozó belső szabályozás és hatályba lépésének dátuma	

7. számú melléklet

Személyes adat továbbításra vonatkozó nyilvántartás

Sorszám	Adattovábbítás időpontja	Érintett neve	Személyes adat továbbításának címzettje	Továbbított személyes adatok köre	Adattovábbítás jogalapja
1.					
2.					
3.					
4.					
5.					

8. számú melléklet

Adatvédelmi incidenskezelési eljárásrend

Jelen melléklet egy átfogó informatikai eljárásrendet tartalmaz, mely az adatvédelmi incidensek kezelésének rendjét szabályozza az Adatkezelőnél. Az eljárásrend meghatározza az incidensek fajtáit, az érintettek kötelezettségeit, az incidenskezelés folyamatát és az incidens elhárítása utáni dokumentáció rendjét is. Az eljárásrend célja, hogy az adatvédelmi incidensek felismerése, a kockázatbecslés, a veszélyre való reagálás gyors és szakszerű legyen. Fontos célkitűzés továbbá, hogy a jövőbeni incidensek elkerülhetővé váljanak, ne ismétlődhessenek meg újra. A szabályozási kör kiterjed az Adatkezelő informatikai rendszereire, a kezelt személyes adatokra, az informatikai rendszerekhez kapcsolódó felhasználók eszközeire és magukra a felhasználókra is.

Adatvédelmi incidens esetén az informatikai feladatok ellátásáért felelős egység vezetője vagy beosztott munkatársa haladéktalanul értesítendő telefonon vagy e-mailen keresztül.

Az incidensek felismerése több csatornán keresztül is történhet. Elsődleges szűrőként az informatikai feladatok ellátásáért felelős egység monitoring rendszere szolgál, de emellett az incidens felismerése és bejelentése a felhasználók részről, szervezeten kívülről (pl.: GOVCERT), vagy egyébként a szolgáltatások minőségének romlásából, lassulásából, kihagyásából is történhet. A felfedezett incidenseket az informatikai feladatok ellátásáért felelős egység megfelelően dokumentálja.

Az incidensek súlyosságát tekintve 3 osztályba sorolandóak aszerint, hogy milyen és mennyi adatot érint vagy az informatikai rendszerek biztonságos működését mennyire befolyásolják. A kockázat meghatározását a lehető leghamarabb el kell végezni.

Magas kockázat: hatását és valószínűségét tekintve nagymértékű káresemény következhet be (az Adatkezelőtől adatok nagy mennyiségben kerülhetnek ki, tűnhetnek el, sérülhetnek, adatvagyon helyreállíthatatlanul megsérülhet, nagyobb vagy azt meghaladó anyagi kár, informatikai rendszerek tartós leállása várható, bizalomvesztés a szervezet iránt)

Közepes kockázat: hatását és valószínűségét tekintve mérsékelt mértékű káresemény következhet be (előző események enyhébb fokon valósulnak meg, a kár mértéke kisebb)

Alacsony kockázat: hatását és valószínűségét tekintve minimális mértékű káresemény következhet be (előző események legenyhébb fokon következhetnek be, a kár maximális mértéke elhanyagolható)

A felfedezett informatikai sebezhetőségek nem számítanak adatvédelmi incidensnek. Az informatikai feladatok ellátásáért felelős egység folyamatosan vizsgálja a sebezhetőségeket, és ha talál olyat, azt közli az érintett felhasználókkal és köteles a sebezhetőségek kijavítására, a kockázatok csökkentése érdekében. Ezzel összefüggésben lekapcsolhat, karanténba helyezhet az informatikai hálózatról eszközöket.

Az adatvédelmi incidens kezelése során közreműködők feladatai és kötelezettségei:

Incidens elhárításáért felelős vezető: az informatikai feladatok ellátásáért felelős egység üzemeltetésért felelős osztályvezetője. Kötelessége az incidenssel kapcsolatos adatok összegyűjtése, védekezés megszervezése, incidens elhárítása, hatékony kommunikáció folytatása az érintettekkel, jelentés írása a vizsgálat alatt és után.

Incidens elhárítási szakember: az informatikai feladatok ellátásáért felelős egység megbízott és szakértelemmel rendelkező alkalmazottja vagy külső szakértő megbízás alapján. Feladatukat a felelős vezető utasításainak megfelelően kötelesek ellátni.

Felhasználó: azon személy, aki jogosultsággal rendelkezik az informatikai rendszerekhez és őt az incidens érintheti. Köteles az incidens elhárításban közreműködő személyek utasításait betartani.

Incidenskezelési csoport: súlyos hatású adatvédelmi incidensek esetén az érintett osztályvezetők, az incidens elhárításáért felelős vezető, szakértők, egyéb külső felek által alkotott csoport, melynek célja az összetett incidens gyors és hatékony megoldása.

A tájékoztatás és információcsere legfőbb fóruma.

Az incidenskezelés további fejlődése érdekében az alkalmazott eljárásokat időközönként vizsgálat alá kell vonni.

Incidenskezelési szakaszok:

1. Felkészülés: a megfelelő felkészültség segítséget nyújt a rendszer gyors visszaállításához, minimalizálja az incidens hatásait és növeli az érintettek bizalmát az Adatkezelő iránt. A felkészülés során azokat a körülményeket kell biztosítani, amelyek lehetővé teszik az informatikai feladatok ellátásáért felelős egység számára az incidensek szakszerű és gyors kezelését (ide tartozik a szabályozási környezet megfelelő kialakítása, eszközök beszerzése, szerepek pontos ismerete, incidenskezelés folyamatának pontos ismerete, kommunikációs csatornák kialakítása, stb.). A felkészülés továbbá azt is jelenti, hogy az incidens kezelésében érintett felek megfelelő tájékozottsággal rendelkeznek az incidensek elhárításával kapcsolatban. A korábbi incidensek elemzése nagy segítséget nyújthat a jövőbeni felkészülés szempontjából. Az alábbi megelőzési célzatú lépések megtételére van szükség:

- Kritikus informatikai rendszerek, adatok, eszközök meghatározása
- Előreláthatólag mire fog irányulni a jövőbeni incidens
- Megfelelő védelmi intézkedések megtétele az információ birtokában
- Tudatosság erősítése a felhasználók irányában
- Annak meghatározása, hogy az adott incidens mekkora hatással lesz a szervezetre

Ezen lépések után a veszélyeknek való kitettség elemezhető. Cél a kockázatokkal arányos védelem kialakítása.

2. Észlelés: az észlelés az incidensgyanús esemény felfedezése, amely történhet a monitoring rendszer riasztása által, felhasználók jelzése által, külső fél felhívása által. Ebben a szakaszban kerül megállapításra, hogy történt-e incidens és hogy az milyen besorolásba kerül. Ennek érdekében szükséges:

- Teljes körű naplózás
- A monitoring rendszer megfelelő beállítása, hogy az esemény azonnal észlelhető legyen
- A monitoring tevékenység folyamatos és hatékony ellátása
- Könnyen hozzáférhető előzmények a log-okban
- A releváns log-ok összegyűjtése és értelmezhető formában való megjelenítése a későbbi vizsgálatok céljából

Ebben a szakaszban kell meghatározni a következőket:

- Besorolás: az incidens veszélyessége alapján (magas, közepes, alacsony)

- Prioritások meghatározása: a magasabb veszélyességi besorolású incidens megelőzi az alacsonyabb szintűt. Azonos szintű incidensek esetén a körülmények szerinti egyedi prioritási sorrend kerül megállapításra

- Szignálás: az incidens kezelésének megfelelő személyre való terhelése

A monitoring rendszer az alábbi részekből tevődik össze:

- Biztonsági szoftverek (pl.: tűzfal, antivírus, spam-szűrő, fájl integritást vizsgáló szoftver stb.)

- Logok (pl.: tűzfal, router logok, operációs rendszer logjai, szolgáltatások, programok logolása, hálózati eszközök és forgalom logolása, webszerver, DNS, DHCP, e-mail előzmények, épületbe való be- és kiléptetés logjai, stb.)

- Nyilvánosan hozzáférhető információ (pl.: új exploitok hírei, IT workshopokon történő információcsere, GOVCERT-ek figyelmeztetései, stb.)

- Belső felhasználók jelzései

- Külső partnerek jelzései (pl.: ügyfelek, internet-szolgáltatók, beszállítók, stb.)

A megfelelően kialakított monitoring-rendszer az alábbiakat állapítja meg:

- Az incidens-gyanús esemény beazonosítása

- Minden releváns információ elemzése az incidenssel kapcsolatban

- Az incidens fajtájának meghatározása (pl.: DDOS támadás, social engeneering, malware támadás stb.)

- Visszaigazolás arról, hogy valóban támadás érte a szervezetet vagy legálabb megpróbálkoztak azzal.

A felhasználók az alábbi magatartásokat kötelesek tanúsítani:

- Incidensgyanús események bejelentése (pl.: nem tudnak bejelentkezni, nem csatlakoznak az informatikai hálózatokhoz, gyanús programokat észlelnek az eszközökön, nem férnek hozzá jogosultságuk szerinti adatokhoz, korrupt adatok gyanúja stb.)

- Minden fontos körülményt kötelesek feljegyezni, arról beszámolni (pl.: mit tapasztalt, mikor tapasztalta, felugró hibaüzenetek tartalma, egyéb furcsaságok, stb.)

- Kötelesek megvárni a szakértők beavatkozását, nem kísérelhetik meg saját maguk a problémák megoldását (ami nagyobb bajt is okozhat)

3. Elszigetelés: az elszigetelés (karantén) alkalmával azonosításra kerül az incidenssel érintett rendszer vagy eszköz, mely során az eszközhöz rendszerhez való hozzáférés erősen korlátozott, továbbá az érintett feleket is tájékoztatja az informatikai feladatok ellátásáért felelős egység a korlátozásokkal kapcsolatban. Ez a szakasz előkészíti a bizonyítékok összegyűjtését, valamint a helyzet további romlásának megakadályozását. Az elszigetelést lehetőleg úgy kell megvalósítani, hogy a rendes üzletmenet folytatható legyen.

Az elszigetelés lehetséges megvalósulási formái:

- jogosulatlan belépés blokkolása
- gyanús email címek és weboldalak blokkolása
- meghatározott portok letiltása
- rendszergazdai jelszó megváltoztatása, ha gyanú merül fel annak kompromittálódásáról
- tűzfal rekonfigurálása
- eszközök fizikai izolációja

Az elszigetelésre az alábbi kritériumok miatt van szükség:

- káresemények további megelőzése
- további adatlopások, módosítások, törlések megakadályozása
- fennmaradó biztonságos informatikai szolgáltatás nyújtása
- megfelelő időtartam biztosítása a stratégiák és eszközök alkalmazásához
- annak biztosítása, hogy az incidenskezelés hatékony lesz
- kockázatok csökkentése, a támadó esetleges válaszlépésének megakadályozása
- bizonyítékok megőrzése a további vizsgálatok céljából

A hiteles bizonyítékok összegyűjtését az alábbi eljárás szerint kell végezni:

- releváns információ azonosítása
- a bizonyíték felfedezőjének neve, beosztása
- felfedezés időpontja
- a bizonyíték megfelelő tárolási helyének meghatározása

4. Kivizsgálás: a kivizsgálás alkalmával az informatikai feladatok ellátásáért felelős egység szakemberei meghatározzák az incidens által elérni kívánt célt, annak kiterjedését és azt a körülményt, ami lehetővé tette az incidens megvalósulását.

A kivizsgálás során az alábbi kérdésekre keressük a választ:

- Ki vagy kik támadták meg a szervezetünket?
- Mi a támadás célja, hatásterülete?
- Mikor történt a támadás?
- Mit akarhatnak tőlünk a támadás elkövetői?
- Miért támadták meg pont a mi szervezetünket?
- Hogyan fordulhatott elő a támadás?
- Milyen módszerrel hajtották végre a támadást?

A feltett kérdések alapján meg kell határozni azon adatok körét, amelyet jogosulatlanul letöltöttek, töröltek, ill. módosítottak.

5. Kármentesítés: a kármentesítés az incidens megtörténte utáni helyreállítási, javítási folyamatot jelenti. Az érintett rendszerek, eszközök itt kerülnek helyreállításra. A folyamat során az informatikai feladatok ellátásáért felelős egység utasításokat adhat az érintett feleknek a kármentesítés hatékonyabb rendezése érdekében. Itt kerül megállapításra továbbá az is, hogy a veszély megszűnt az intézkedések következtében.

A kármentesítési eljárásban a következő pontokat kell szem előtt tartani:

- az érintett rendszerek és eszközök pontos ismerete az incidens közvetlen megszüntetése előtt
- incidens elhárítására hozott döntés végrehajtása
- malware-analízis újbóli lefuttatása
- reakció figyelése a támadó felől
- megfelelő időn keresztüli monitoring, hogy minden a normál üzletmenet szerint folyik

Ennek megfelelően rendelkezni kell visszaállítási tervvel, mely tartalmazza:

- a fertőzött rendszerek visszaállítását (pl.: lemezképből)
- fertőzött fájlok visszaállítását (pl.: korábbi mentésből)
- a karantén megszűntetésének lépéseit
- érintett felhasználók jelszavainak megváltoztatását
- biztonsági frissítések alkalmazását
- rendszer alapos biztonsági tesztelését
- annak megerősítését, hogy az informatikai rendszerek a továbbiakban biztonságosak

A hatékony incidens-kezelést gyorsan és pontosan kell elvégezni, a támadó válaszlépését időben és lehetőségekben is ki kell zárni.

6. Utólagos elemzés: az incidens során kinyert adatok, információk elemzésre kerülnek. Ez segít hatékonyabbá tenni a jövőbeni folyamatokat és szabályozásokat. Segíti továbbá a hibákból való tanulást és azt, hogy az incidens többé ne ismétlődhessen meg. Az utólagos elemzést a szervezetünk megküldi a felettes szervünknek és a többi társ-szervezetnek is, a hatékonyabb védekezés elősegítése és információk megosztása céljából.

Az utólagos elemzés célja a következő:

- megfelelő vizsgálat lefolytatása a támadó kilétének megállapítása érdekében
- problémaközpontú elemzés végrehajtása (miért történhetett meg az incidens)
- az incidens szervezetre gyakorolt hatásának felmérése (károk összesítése)
- esetleges büntetőeljárás lefolytatásának támogatása

Ennek megvalósulása érdekében a végső jelentés tartalmazza:

- az incidens természetének teljes leírását, események kronológiai sorrendjét, milyen intézkedések történtek az incidens elhárítása érdekében

- a ráfordított költségek összegét, a kiesett bevételek nagyságának becslését, a jó hírnév sérülését, esetleges hiányosságok feltárását

- javaslatokat azzal kapcsolatban, hogy a jövőbeni hasonló események megelőzhetőek, észrevehetőek és hatékonyabban kezelhetőek legyenek

A végső jelentés az alábbi kérdésekre is keresi a választ:

- Milyen jól teljesített az incidens elhárításáért felelős személy, csoport?

- Követték-e az incidensek kezelésére meghatározott folyamatok előírásait?

- Elégnek bizonyult-e a leírások követése?

- Milyen információra lett volna hamarabb szükség?

- Volt-e olyan lépés a folyamatba, ami talán késleltette az incidens elhárítását?

- Megelőzhetőek lettek-e volna az előre nem látott események?

- Mi az, amit az incidens elhárításában közreműködő személyek, csoport másként csinálna legközelebb?

- Hogyan lehetne az információk megosztását más szervezetekkel optimalizálni?

- Milyen intézkedések szükségesek ahhoz, hogy a jövőben hasonló incidensek ne fordulhassanak elő?

- Milyen prekurzorokat és indikátorokat kell figyelni a jövőben hasonló incidens megelőzése céljából?

- Hogyan lehet a megállapításokat a szervezet kockázatértékelési folyamatába beleültetni?

- Mi az a tanulság, amit az incidens után levonhatunk magunknak?

9. számú melléklet

Tájékoztatás ellenőrzésről

Tisztelt ……! (szervezeti egység vezetője)

Ezúton tájékoztatom, hogy ……. (munkáltatói érdek megnevezése) miatt a Munka törvénykönyvéről szóló 2012. évi I. törvény 11/A. § (3) bekezdése alapján ellenőrzésre kerül sor …… napján / …….. közötti időszakban.

Ellenőrzött szervezeti egység/személy(ek):

- ……..
- ……
- ……..

Az ellenőrzés célja:
……
……
……

Az ellenőrzés vezetésével ……. (név, beosztás) közalkalmazottat bíztam meg.

Az ellenőrzési eljárás menete:
……
……
……

Az ellenőrzött személy jogai/jogorvoslati lehetőségei:
……
……
……

Budapest, 2019. ……..

Üdvözlettel:

Láng István
főigazgató /

……
igazgató

10. számú melléklet

Tájékoztatás kamerás megfigyelésről

Tisztelt Látogató / Kolléga!

A munkahelyi kamerás megfigyeléssel kapcsolatban, az alábbiakról tájékoztatom Önt:

- az adatkezelés jogalapja:
- egyes kamerák elhelyezése (látószög, célok, terület, tárgy, közvetlen vagy rögzített megfigyelés valósul-e meg):
- az üzemeltető személy meghatározása:
- a felvételek tárolásának ideje, helye:
- adatbiztonsági intézkedések:
- megismerésre jogosult személyek köre:
- a felvétel továbbításának lehetősége:
- a felvételek a munkáltató által milyen célra használható fel:
- a munkavállalókat / a látogatókat megillető jogok, azok gyakorlásának módja:
- az információs önrendelkezési jogok megsértése esetén rendelkezésre álló jogérvényesítési eszközök:

Tisztelettel:

Országos Vízügyi Főigazgatóság /
…….. Vízügyi Igazgatóság