36300/142-5/2016. ált.

VESZPRÉM MEGYEI KATASZTRÓFAVÉDELMI IGAZGATÓSÁG

A VESZPRÉM MEGYEI KATASZTRÓFAVÉDELMI IGAZGATÓ

5/2016. számú

INTÉZKEDÉSE

a Veszprém Megyei Katasztrófavédelmi Igazgatóság Adatvédelmi és Adatbiztonsági Szabályzatáról

Veszprém, 2016. február „26"

Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.), valamint a 1/2016. számú BM OKF főigazgatói utasítás (a továbbiakban: OKF Szabályzat) alapján kiadom a Veszprém Megyei Katasztrófavédelmi Igazgatóság (a továbbiakban: Veszprém MKI) Adatvédelmi és Adatbiztonsági Szabályzatáról szóló

i n t é z k e d é s t:

Az intézkedés hatálya kiterjed a Veszprém MKI teljes szervezetére és személyi állományára.

I.
A Szabályzat kibocsátásának célja

A Szabályzat kibocsátásának célja, hogy a Veszprém MKI a működése során az információs önrendelkezési jog érvényesülését biztosítsa, továbbá a kezelt személyes adatok jogosulatlan felhasználásának megakadályozása érdekében a személyes adatok védelmének, valamint a közérdekű és közérdekből nyilvános adatok nyilvánosságának és megismerhetőségének biztosítása megvalósuljon, különös tekintettel a helyi sajátosságokra.

II.
Az adatkezelés alapelvei

1. A Veszprém MKI személyi állományának tagjai a szolgálati feladataik ellátása körében személyes adatot csak a vonatkozó jogszabályok és belső normák, az OKF Szabályzat, valamint jelen intézkedés előírásainak figyelembevételével kezelhetnek.

2. Személyes adat kizárólag pontosan meghatározott jogszerű célból, jog gyakorlása és kötelezettség teljesítése érdekében kezelhető. Az adatkezelésnek minden szakaszában meg kell felelnie a célhoz kötöttség elvének.

3. Személyes adatot jogszabályi felhatalmazás hiányában az érintett hozzájárulása alapján lehet kezelni.

III.
Az adatkezelést, illetve adatfeldolgozást végző szervek elhelyezésére szolgáló helyiségek kialakítása során irányadó adatbiztonsági előírások, az illetéktelen hozzáférés megakadályozása érdekében alkalmazandó helyi védelmi intézkedések

1. Fizikai biztonság

1.1. A hivatásos katasztrófavédelmi szervek objektumait el kell látni a szükséges vagyon- és tűzvédelmi eszközökkel, amelyet a mindenkor hatályos **Tűzvédelmi Szabályzat** részletez.

1.2. Az irodákban, egyéb helyiségekben az adathordozók közvetlen tárolására szolgáló berendezési tárgyak is az adatok biztonságát szolgálják. Az ügyirat jellegétől függően a tárolás a zárt irodában elhelyezve, zárható szekrényben, lemezszekrényben, vagy páncélszekrényben történik. Személyes adatokat tartalmazó iratokat csak lezárt szekrényben szabad tárolni.

2. Adatbiztonság

2.1. Az adatkezelő, illetve tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek az adatvédelmi szabályok érvényre juttatásához szükségesek.

2.2. A különböző nyilvántartásokban elektronikusan kezelt adatállományok védelme érdekében megfelelő technikai megoldással biztosítani kell, hogy a nyilvántartásokban tárolt adatok – kivéve, ha azt törvény lehetővé teszi – közvetlenül ne legyenek összekapcsolhatók és az érintetthez rendelhetők.

2.3. Adatbiztonsági előírások, adatbiztonsági fokozatok:

2.3.1. Az adatbiztonsági intézkedések meghatározása érdekében a hivatásos katasztrófavédelmi szervek kezelésében lévő minden egyes személyes adatot tartalmazó adatállományt az adatállományt kezelő szervezeti elem vezetőjének a védelmi igény szempontjából értékelni kell, majd a 2.3.2. pontban meghatározott biztonsági fokozatba kell sorolni. A besorolásban a belső adatvédelmi felelős szükség esetén segítséget nyújt.

2.3.2 A hivatásos katasztrófavédelmi szervek adatkezelésének biztonsági fokozatai:

a) Alap adatbiztonsági fokozat: Alapesetben azon adatkezelések tartoznak ebbe a fokozatba, amelyekben feldolgozott adatok közérdekből nyilvános adatok.

b) Fokozott adatbiztonsági fokozat: Alapesetben azon adatkezelések tartoznak ebbe a fokozatba, amelyekben személyes adatok találhatóak.

c) Kiemelt adatbiztonsági fokozat: Alapesetben ebbe a fokozatba tartoznak a különleges adatot tartalmazó adatkezelések.

Amennyiben egy adatállományban többféle besorolású adat található, a teljes adatállományt a magasabb adatbiztonsági kategóriába kell sorolni.

3. Informatikai Adatbiztonság

3.1. A Veszprém MKI mint adatkezelő gondoskodik az adatok biztonságáról. Az adatokat megfelelő intézkedésekkel védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen.

3.2. A Veszprém MKI-nak az adatok biztonságát szolgáló intézkedések meghatározásakor és alkalmazásakor tekintettel kell lennie a technika mindenkori fejlettségére. Több lehetséges adatkezelési megoldás közül azt kell választani, amely a személyes adatok magasabb szintű védelmét biztosítja.

3.3. Az adatbiztonsági rendszabályok érvényesítése érdekében a szükséges intézkedéseket meg kell tenni mind a manuálisan kezelt, mind a számítógépen tárolt és feldolgozott személyes adatok biztonsága érdekében.

3.4. A Veszprém MKI a tulajdonát képező informatikai eszközökön folytatott Internet használatot figyeli, naplózza. A Veszprém MKI kijelölt szakemberei ezekbe az információkba betekinthetnek és kezelhetik azokat.

3.5. A levelezőrendszerből külsős címzett részére küldött üzenetek láblécében – jelen szabályzattal és az Informatikai Biztonsági Szabályzattal összhangban álló – standard tájékoztató üzenetet kell feltüntetni, mely eligazítást ad az üzenet fogadója részére az abban foglalt információk jellegét tekintve, illetve a téves kézbesítés esetére.

3.6. Informatikai nyilvántartások védelme:

A Veszprém MKI (mint adatkezelő) az informatikai védelemmel kapcsolatos feladatai körében gondoskodik különösen:

3.6.1. A jogosulatlan hozzáférés elleni védelmet biztosító intézkedésekről, ezen belül a szoftver és hardver eszközök védelméről, illetve a fizikai védelemről (hozzáférés védelem, hálózati védelem).

3.6.2. Az adatállományok helyreállításának lehetőségét biztosító intézkedésekről, ezen belül a rendszeres biztonsági mentésről és a másolatok elkülönített, biztonságos kezeléséről.

3.6.3. Az adatállományok vírusok elleni védelméről (vírusvédelem).

3.6.4. Az adatállományok, illetve az azokat hordozó eszközök fizikai védelméről, ezen belül a tűzkár, vízkár, villámcsapás, egyéb elemi kár elleni védelemről, illetve az ilyen események következtében bekövetkező károsodások helyreállíthatóságáról (archiválás, tűzvédelem).

3.6.5. Hozzáférés-védelem: az adathozzáféréshez csak érvényes, személyre szóló, azonosítható jogosultsággal lehet hozzáférni. Hálózati erőforrásokhoz csak érvényes felhasználói névvel és megfelelő biztonsági szintű jelszóval lehet hozzáférni. A jelszavak cseréjéről rendszeresen gondoskodni kell. Az állomány tagjai részére, az általuk használt számítógépen kötelező a jelszavas képernyőkímélő program alkalmazása.

3.7. Hálózati védelem: a mindenkor rendelkezésre álló számítástechnikai eszközök felhasználásával meg kell akadályozni, hogy adatokat tároló, hálózaton keresztül elérhető szerverekhez illetéktelen személy hozzáférjen.

3.8. Nyomonkövetés, naplózás: Számítógépes adatállomány rendszerbe állítása esetén az adattovábbítás naplózását programtechnikailag vagy manuálisan (papír alapon) biztosítani kell. Manuális adatkezelések esetén – vagy ha a számítógépes adatkezeléseknél a naplózás nem biztosítható – manuális módon (például betekintő lap vezetésével) kell gondoskodni az adattovábbítási nyilvántartás vezetéséről.

3.9. Papíralapú nyilvántartások védelme

A Veszprém MKI (mint adatkezelő) a papíralapú nyilvántartások védelme érdekében megteszi a szükséges intézkedéseket különösen a fizikai biztonság, illetve tűzvédelem tekintetében.
A munkavállalók, és egyéb, a Veszprém MKI érdekében eljáró személyek az általuk használt, vagy birtokukban lévő, személyes adatokat is tartalmazó adathordozókat, függetlenül az adatok rögzítésének módjától, kötelesek biztonságosan őrizni, és védeni a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés ellen.

IV.
A területi belső adatvédelmi felelős feladat- és hatásköre

1. Az adatvédelmi felelős eljár a részére átruházott – és munkaköri leírásában rögzített – adatvédelemmel összefüggő feladatkörökben, az adatkezelő szerv vezetője ugyanakkor továbbra is felelős az adatkezelés jogszerűsége érdekében hatáskörébe tartozó intézkedések megtételéért. A területi belső adatvédelmi felelős adatvédelmi feladatainak gyakorlása során az őt kinevező vezető közvetlen alárendeltségébe tartozik.

a) segíti az adatkezelő szerv vezetőjét a katasztrófavédelemi adatkezelésre vonatkozó jogszabályok és belső normák érvényre juttatásában, figyelemmel kíséri az adatvédelemmel összefüggő jogszabály-változásokat, előkészíti az adatkezelő szerv vezetőjének adatvédelmi tárgyú döntéseit;
b) kivizsgálja a területi és helyi szerv adatkezelésével összefüggésben érkező panaszokat, kifogásokat, közreműködik, illetve segítséget nyújt az érintettek jogainak gyakorlásában;
c) az adatkezelő szerv vezetőjének megbízásából ellenőrzi az adatkezelő szervnél, illetve az alárendelt adatkezelő szerveknél az adatvédelmi követelmények megtartását, az előírások megszegésének észlelése esetén felhív a jogszerű állapot haladéktalan helyreállítására és a hiányosságokat jelzi a szerv vezetőjének, és indokolt esetben a szerv vezetőjénél kezdeményezi a felelősség megállapításához szükséges eljárás lefolytatását;
d) gondoskodik a területi és helyi szerv személyi állományának oktatásáról;

e) elkészíti az adatkezelő szerv adatvédelmet érintő belső normáinak tervezetét, jelzi a jogalkalmazás során tudomására jutott, esetleges normamódosítást igénylő problémákat;
f) vezeti az adatkezelő szerv adatvédelmi és adattovábbítási nyilvántartását;
g) a kérelem tárgyában érintett szakterület közreműködésével elkészíti az érintettnek a személyes adatai kezelésére vonatkozó kérelmére, illetve a közérdekű adat megismerésére irányuló kérelmekre adandó válasziratokat;
h) rendszeresen ellenőrzi a területi adatkezelő szerv közzétételi listáinak naprakészségét és teljességét;
i) felügyeli az adatkezelő szerv adatszolgáltatási tevékenységét, különös tekintettel a nemzetközi együttműködés keretében továbbítandó személyes adatokra, felkérésre adatvédelmi szempontból állást foglal az adatok továbbításának jogszerűségével kapcsolatban;
j) évente február 28-ig jelentésben értékeli a területi és helyi szerv adatvédelmi és adatbiztonsági helyzetét;
k) végzi a NAIH felé az adatvédelmi nyilvántartásába történő bejelentésekkel összefüggő feladatokat;
l) végzi a személyes adatok kezelése és feldolgozása kapcsán tájékoztatás iránt benyújtott elutasított kérelmekkel, továbbá az elutasított közérdekű adat-megismerési igényekkel kapcsolatos tájékoztatást;
m) ellátja az Egységes Közadatkereső Rendszerrel valamint a Központi Jegyzékkel kapcsolatos, jogszabályban meghatározott feladatokat;
n) az adatvédelmi felelős egyben jogtanácsos, így a peres képviseletet ellátja adatvédelmi tárgyú perekben;
o) összesíti az adatvédelmi incidensek nyilvántartását, a szakterületek által havonta készített táblázatos kimutatás alapján;
p) ellátja mindazon feladatokat, amelyeket a területi adatkezelő szerv Adatvédelmi és Adatbiztonsági Szabályzata részére feladatként meghatároz.

2. A területi adatvédelmi felelős által készített, NAIH felé az adatvédelmi nyilvántartásába történő bejelentésekkel kapcsolatban meghatározott jelentés tartalmazza különösen:

a) az adatkezelő szerveknél végzett adatvédelmi tárgyú ellenőrzések megjelölését, azok fontosabb megállapításait, a feltárt lényeges szabálytalanságokat, hiányosságokat, a megszüntetésükre tett intézkedéseket;
b) az adatkezelő szervek állományába tartozók ellen az adatvédelmi előírások megsértése miatt indított fegyelmi, szabálysértési és büntetőeljárásokra vonatkozó adatokat (az érintettek megjelölése nélkül);
c) az adatkezelő szerveknél lefolytatott oktatások, továbbképzések gyakorlatát;
d) a NAIH által végzett helyszíni vizsgálatokat, megkereséseket, azok fontosabb megállapításait;
e) a közérdekű adatok nyilvánosságának egyedi kérelmek útján és honlapon történő közzététellel biztosított helyzetét az adatkezelő szervnél, ideértve a NAIH felé küldött éves tájékoztató megtörténtét;
f) az Adatvédelmi Nyilvántartásba tett bejelentések számát;
g) az elvégzett honlap ellenőrzések számát, eredményét;
h) az adatvédelem és információszabadság területén adódott egyedi ügyeket.

3. Az adatvédelmi felelős ellenőrzése kiterjedhet különösen a számítógépes munkaállomások jelszóval történő védelmére, az irodában hozzáférhető dokumentumok személyes adat tartalmára,

valamint az Intézkedésben meghatározottakra. A területi adatvédelmi felelős ellenőrzéseit hivatali munkaidőben, valamint azon túl is végezheti.

4. Az irodában minden olyan dokumentum hozzáférhetőnek tekintendő, amely elöl található, vagy nem elzárt szekrényben van.

V.
Az adatkezelés szabályai
1. Általános szabályok

1.1. Az alkotmányos védelem elvének megfelelően a hivatásos katasztrófavédelmi szervek adatkezelése törvényi felhatalmazáson vagy az érintett hozzájárulásán alapulhat.

1.2. Amennyiben a személyesadat-kezelést nem törvény vagy önkormányzati rendelet rendeli el, az adatfelvételt belső szabályozóval vagy egyéb írásos formában kell elrendelni. Erre a területi szerv vezetője, helyi szintű adatkezelés esetén a katasztrófavédelmi kirendeltség vezetője jogosult.

1.3. Személyesadat-kezelési kötelezettséget előíró belső szabályozó vagy írásbeli döntés előkészítése során be kell szerezni – a szolgálati út betartásával, a területi belső adatvédelmi felelős bevonásával – a BM OKF belső adatvédelmi felelősének írásbeli véleményét.

1.4. Az érintett kérelmére indult eljárásban a szükséges adatainak kezeléséhez történő hozzájárulását vélelmezni kell. Erre a tényre az érintett figyelmét az eljárás kezdetén fel kell hívni.

1.5. A hozzájárulást – későbbi igazolhatósága érdekében – különleges adatnak nem minősülő személyes adatok esetén is írásban kell rögzíteni. Nem kell írásban rögzíteni a hozzájáruló nyilatkozatot, ha az érintett mindennapi életben előforduló helyzetben ad – akár ráutaló magatartással is – az adatkezelésre vonatkozó félreérthetetlen hozzájárulást.

1.6. A tűz elleni védekezésről, a műszaki mentésről és a tűzoltóságról szóló 1996. évi XXXI. törvény (a továbbiakban: Ttv.) 10/A.§ rendelkezéseinek megfelelően a segélyhívás, valamint a tűzjelzés fogadásakor a jelzésfogadó törvényi felhatalmazás alapján az alábbi adatokat rögzítheti:

a) a bejelentő nevét,
b) a bejelentő telefonszámát, ennek hiányában lakcímét,
c) a bejelentéskor használt telefonszámhoz tartozó előfizető nevét, címét,
d) a bejelentő által használt telefonállomás azonosított adatait,
e) a hívások rögzített tartalmát, a tűzoltási, műszaki mentési feladatot indokoló esemény helyét és jellegét, a személyi sérülés, haláleset adatait,
f) a műveletirányítás által szükségesnek tartott további, személyes adatnak nem minősülő információt.

1.7. A kárhelyszínen beavatkozó állomány a Ttv. 10/A.§ (2) bekezdésében szabályozottak alapján a helyszínen tartózkodó, a káreseménnyel kapcsolatban érdemi információval szolgálni tudó személyek alábbi személyes adatait rögzítheti törvényi felhatalmazás alapján:

a) név,
b) lakcím,

c) egyéb elérhetőség.

1.8. A személyes adatok automatizált feldolgozása során az adatkezelő és az adatfeldolgozó 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 azt hogy
f) az automatizált feldolgozás során fellépő hibákról jelentés készüljön.

1.9. Az érintettet az adatkezeléshez történő hozzájárulásának beszerzése előtt tájékoztatni kell arról, hogy:

a) milyen adatait, milyen célból, mennyi ideig kívánja kezelni az adatkezelő hivatásos katasztrófavédelmi szerv;
b) mely hivatásos katasztrófavédelmi szerv és hol végzi az adatkezelést, illetve adatfeldolgozó igénybevétele esetén mely adatfeldolgozó és hol végzi az adatfeldolgozást;
c) az adatok továbbítására milyen célból és mely szervek részére kerülhet sor;
d) az érintett az adatkezeléssel kapcsolatban milyen jogokkal rendelkezik (tájékoztatás-kérési, helyesbítési és törléskezdeményezési, valamint tiltakozási jog);
e) milyen jogorvoslati lehetőséggel rendelkezik (NAIH- hoz fordulás, bírósági jogérvényesítés útja).

1.10. Az érintettek tájékoztatása az adatkezelést végző szervezeti elem kötelezettsége.

1.11. Ha az érintettek személyes tájékoztatása lehetetlen vagy aránytalan költséggel járna, a tájékoztatás megtörténhet az alábbi információknak az adatkezelő hivatásos katasztrófavédelmi szerv honlapján történő nyilvánosságra hozatalával is:

a) az adatgyűjtés ténye,
b) az érintettek köre,
c) az adatgyűjtés célja,
d) az adatkezelés időtartama,
e) az adatok megismerésére jogosult lehetséges adatkezelők személye,
f) az érintettek adatkezeléssel kapcsolatos jogainak és jogorvoslati lehetőségeinek ismertetése, valamint,
g) ha az adatkezelés adatvédelmi nyilvántartásba vételének van helye, az adatkezelés nyilvántartási száma.

1.12. Aki a munkáltató által végzett adatkezelés kapcsán saját személyes adatai tekintetében adatvédelmi incidens bekövetkezését észleli, jogosult azt közvetlenül jelezni a BM OKF belső adatvédelmi felelősének.

1.13. A belső adatvédelmi felelős a neki bejelentett és a saját hatáskörben észlelt, valamint a szakterület által havonta leadott – adatvédelmi incidenseket tartalmazó – táblázatokból nyilvántartást vezet, amely tartalmazza az érintett személyes adatok körét, az adatvédelmi incidenssel érintettek körét és számát, az adatvédelmi incidens időpontját, körülményeit, hatásait és az elhárítására megtett intézkedéseket, valamint az adatkezelést előíró jogszabályban meghatározott egyéb adatokat.

A bekövetkezett adatvédelmi incidensek tekintetében a következmények elhárításának módjára a belső adatvédelmi felelős tesz javaslatot.

2. Belső adatvédelmi nyilvántartás

2.1 Az adatkezelő hivatásos katasztrófavédelmi szerv belső adatvédelmi felelőse legkésőbb az adatkezelést a megkezdése előtti tizennegyedik napig köteles belső adatvédelmi nyilvántartásában rögzíteni legalább az adatkezelés alábbi adatait:

a) az adatkezelés célját,

b) az adatkezelés jogalapját,

c) az érintettek körét,

d) az érintettekre vonatkozó adatok leírását,

e) az adatok forrását,

f) az adatok kezelésének időtartamát,

g) amennyiben az adattovábbítás elvi lehetősége fennáll, a továbbítható adatok fajtáját, címzettjét és a továbbítás jogalapját, ideértve a harmadik országokba irányuló adattovábbításokat is,

h) a tényleges adatkezelés helyét (szervezeti elem és az adatok fizikai helyének megjelölésével,

i) ha az adatkezelő adatfeldolgozót vesz igénybe, az adatfeldolgozó nevét és címét vagy székhelyét, az adatfeldolgozás helyét és az adatfeldolgozónak az adatkezeléssel összefüggő tevékenységét, az alkalmazott adatfeldolgozási technológia jellegét.

Az adatkezelésekben bekövetkezett változást vagy az adatkezelés megszüntetését a bejelentésre kötelezett nyolc napon belül bejelenti a belső adatvédelmi felelősnek.

2.2. A belső adatvédelmi felelőshöz felterjesztett adatkezeléseket a NAIH által vezetett nyilvántartásba – a NAIH által e célból biztosított felületen keresztül:

a) a kötelező adatkezeléseket az adatkezelésre vonatkozó törvény vagy önkormányzati rendelet hatályba lépését követő 20 napon belül,

b) az érintettek hozzájárulásán alapuló adatkezeléseket legkésőbb az adatkezelés megkezdését megelőző 9. napon

a belső adatvédelmi felelős bejelenti.

3. Adattovábbítás a katasztrófavédelemi adatkezelésekből, az adattovábbítási nyilvántartás

3.1. Katasztrófavédelemi adatkezelésekből személyes adatot továbbítani az érintett beleegyezésének, hozzájárulásának hiányában csak törvényben meghatározott szerv vagy személy részére, törvényben meghatározott adatkörben lehet, a célhoz kötöttség elvének maradéktalan érvényesítésével.

3.2. Adatvédelmi szempontból akkor tekinthető az adattovábbítás jogszerűnek, ha a személyes adat birtokában lévő szerv vagy személy jogosult annak továbbítására, az adattovábbítás címzettje (adatkérő) pedig törvényi felhatalmazással vagy az érintett hozzájárulásával rendelkezik az adat kezeléséhez, és az adatkérés célja mindezzel összhangban van.

3.3. Az adattovábbítás fenti két pontban meghatározott feltételeinek meglétét az adatot továbbító adatkezelő minden egyes személyes adattal összefüggésben ellenőrizni köteles.

3.4. A hivatásos katasztrófavédelmi szerv valamennyi szervezeti eleme az általa továbbított személyes adatokról adattovábbítási nyilvántartást vezet.

3.5. Az adattovábbítási nyilvántartásban rögzíteni kell:

a) az érintett nevét;
b) az adatigénylő nevét vagy megnevezését;
c) adatkezelést előíró jogszabályokat, egyéb adatokat;
d) az adattovábbítás teljesítése esetén az adattovábbítás jogalapját, időpontját, címzettjét, továbbított személyes adatok körének meghatározását, a továbbított adatok fajtáját (maguk a szolgáltatott adatok nem képezik az adattovábbítási nyilvántartás részét);
e) az adattovábbítás megtagadása esetén a kért személyes adatok megjelölését és az adattovábbítás megtagadásának indokát.

3.6. A belső adatvédelmi felelős legalább negyedévente köteles ellenőrizni a szerv közzétételi listáinak feltöltöttségét.

3.7. A belső adatvédelmi felelős minden félévben köteles ellenőrizni az adatkezelő szervnél kiosztott hozzáférési jogosultságok aktualizáltságát. Az ellenőrzést az adatvédelmi felelős a szerv rendszergazdájával közösen köteles végrehajtani, annak lefolytatása során a jelszavak meghatározott időszakonkénti megváltoztatására vonatkozó kötelezettség teljesítését is ellenőrizni kell.

3.8. A hivatásos katasztrófavédelmi szerv állományába újonnan került olyan személyeket, akik munkakörüknél fogva személyes adatokat kezelnek, az adatvédelmi felelős – az adatkezelő szerv személyzeti feladatot ellátó szervezeti elemével történő rendszeres egyeztetés alapján – köteles az állományba vételt követő három hónapon belül adatvédelmi oktatásban részesíteni, majd az oktatást követő három hónapon belül vizsgáztatásukat elvégezni.

VI.
Az általános, különös és egyedi közzétételi listák

1. A közérdekű adatok nyilvánossága és az elektronikus információszabadság elvének megfelelően a Veszprém MKI – erre irányuló külön kérelem nélkül – a közérdekű és közérdekből nyilvános adatokat honlapján általános, különös és egyedi közzétételi listák alapján nyilvánosságra hozza.

2. A listák tartalmának honlapon történő elhelyezéséről az érintett szakterületek adatszolgáltatása és közreműködése alapján a honlap szerkesztéséért felelős szóvivő gondoskodik.

3. Jelen intézkedés 1. melléklete tartalmazza a Veszprém MKI közzétételi listáit és a listák egyes részei tekintetében adatszolgáltatásra kötelezett szervezeti elemek megjelölését.

4. A közzétételi listákba feltöltött adatok helytállóságáért és naprakészségéért az adatfelelős szervezeti egység, a kapott adatok feltöltéséért az adatközlő, a listák egyes részei feltöltöttségének ellenőrzéséért a belső adatvédelmi felelős felel.

VII.
Közérdekű adat megismerése iránti kérelmek

1. Közérdekű adat megismerése iránti – bármely formában érkezett – kérelmet soron kívül, de legkésőbb a következő munkanap hivatali munkaidejének végéig meg kell küldeni a belső adatvédelmi felelősnek a veszprem.hivatal@katved.gov e-mail címre a válasz tervezetével együtt.

2. Az elutasított kérelmekről a Veszprém MKI adatvédelmi felelőse - az Infotv. 30.§ (3) bekezdésben meghatározott adattartalmú, jelen intézkedés 2. számú melléklete szerinti - nyilvántartást vezet.

3. Az érintett kérelmének elutasítása esetén az elutasításról adott tájékoztatás kiterjed a bírósági jogorvoslat, továbbá a Nemzeti Adatvédelmi és Információszabadság Hatósághoz fordulás lehetőségére.

4. A Veszprém MKI által kezelt személyes adatok továbbításáról szervezeti egységenként az Infotv. 15.§ (2) bekezdésben meghatározott adattartalommal, jelen intézkedés 3. számú melléklete szerinti adattovábbítási nyilvántartást kell vezetni.

5. Az adatvédelmi felelős a kérelem kézhezvételekor haladéktalanul megvizsgálja, hogy a kérelem teljesítéséhez szükséges alábbi alapvető információk rendelkezésre állnak-e:

a) az igénylő neve vagy megnevezése;

b) az értesítések és a válasz megküldéséhez szükséges elérhetőség;

c) az igényelt adatok pontos meghatározása;

d) nyilatkozat arról, hogy az adatokat részére milyen formában kell rendelkezésre bocsátani;

e) a kötelezettségvállalás a dologi költségek megfizetéséről.

6. Amennyiben az igény nem tartalmazza az igény teljesítéséhez szükséges adatokat – ideértve azt az esetet is, ha az adatigénylő a megismerni kívánt adatot nem tudja pontosan megjelölni – a belső adatvédelmi felelős haladéktalanul, de legkésőbb az igény kézhezvételét követő 3 napon belül felveszi a kapcsolatot az igénylővel és – a tőle elvárható módon és mértékben – segítséget nyújt a megismerni kívánt adatok körének pontos meghatározása érdekében.

7. A belső adatvédelmi felelős a kérelem pontosításának elmulasztása esetén figyelmezteti az adatigénylőt arra, hogy amennyiben a pontosítást elmulasztja, igényének teljesítése részben vagy egészben meghiúsul.

8. Amennyiben az igényelt adat kezelője nem a megkeresett szerv, úgy azt haladéktalanul, de legkésőbb az igény kézhezvételét követő 8 napon belül köteles továbbítani a közérdekű adatot kezelő szervnek. Az igény áttételéről egyidejűleg tájékoztatni kell az igénylőt is.

9. Amennyiben az adatkezelő szerv a megkeresett szerv számára nem azonosítható, továbbá amennyiben a tényleges adatkezelő szerv illetékessége kétséget kizáróan egyértelműen megállapítható volt az adatigénylő számára, az adatkezelő szerv tájékoztatja az igénylőt az áttétel akadályáról vagy felhívja az igénylőt adatigényének az illetékes szervhez történő megküldésére.

10.Amennyiben az igény 15 nap alatt nem teljesíthető, különösen, amennyiben az adatok az igényelt csoportosításban nem állnak rendelkezésre és azok kigyűjtése a határidőn belül objektív okból nem lehetséges, vagy az igény nagyszámú, nagy terjedelmű adatra vonatkozik, valamint, ha az adatigénylés teljesítése a hivatásos katasztrófavédelmi szerv alaptevékenységének ellátásához szükséges munkaerőforrás aránytalan mértékű igénybevételével jár, az ügyintézési határidő további 15 nappal meghosszabbítható. Ebben az esetben igénylőt a belső adatvédelmi felelős az igény kézhezvételétől számított 15 napon belül tájékoztatja a határidő meghosszabbításának okáról és a válasz várható időpontjáról.

11.Az elutasított kérelmekről, valamint az elutasítások indokairól a belső adatvédelmi felelős nyilvántartást vezet, és az abban foglaltakról minden évben január 31-ig tájékoztatja a NAIH-ot.

VIII.
Záró rendelkezések

1. Jelen intézkedés függelékében mintatár található az adatvédelemhez köthető eljárásokra, melyet az adatkezelés során alkalmazni kell.

2. Jelen intézkedés a kiadás napján lép hatályba, rendelkezéseit a teljes személyi állománnyal ismertetni kell.

3. Jelen intézkedés hatályon kívül helyezi a Veszprém Megyei Katasztrófavédelmi Igazgatóság Adatvédelmi és Adatbiztonsági Szabályzatáról szóló 1/2014. számú igazgatói intézkedést.

Dányi Béla tű. ezredes
igazgató

Készült:	1 eredeti példányban
Egy példány:	3 lap (5 oldal)
Készítette:	dr. Lóderer Éva tű. szds.
Kapja:	Irattár
	Szervezeti egységek, kirendeltségek, hivatásos tűzoltó-parancsnokságok
ITSZ:	01-01.006.