BORSOD-ABAÚJ-ZEMPLÉN VÁRMEGYEI
KATASZTRÓFAVÉDELMI IGAZGATÓSÁG
IGAZGATÓ

A BORSOD-ABAÚJ-ZEMPLÉN VÁRMEGYEI KATASZTRÓFAVÉDELMI IGAZGATÓSÁG IGAZGATÓJÁNAK

18/2025. számú

I N T É Z K E D É S E

A Borsod-Abaúj-Zemplén Vármegyei Katasztrófavédelmi Igazgatóság adatvédelmi, adatbiztonsági és közérdekű adatok nyilvánosságára vonatkozó szabályzatáról

Miskolc, 2025. július 10.

Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény 25/A. § (3) bekezdésére, valamint 30. § (6) bekezdésére, a hivatásos katasztrófavédelmi szervek adatvédelmi, adatbiztonsági és közérdekű adatok nyilvánosságára vonatkozó szabályzatáról szóló BM Országos Katasztrófavédelmi Főigazgató 6/2025. (VI. 30.) számú utasításban foglaltak végrehajtása érdekében kiadom az alábbi

i n t é z k e d é s t :

1. Az intézkedés hatálya kiterjed a Borsod-Abaúj-Zemplén Vármegyei Katasztrófavédelmi Igazgatóságra (továbbiakban: BAZ VMKI) valamint a helyi szervekre továbbá mindezek teljes személyi állományára.

2. BAZ VMKI adatvédelmi, adatbiztonsági és közérdekű adatok nyilvánosságára vonatkozó szabályzata (továbbiakban: Szabályzat) jelen intézkedés mellékletét képezi.

3. A Szabályzatot a hatályba lépése napján közzé kell tenni a BAZ VMKI honlapján, az általános közzétételi lista részeként.

4. Jelen intézkedés a kiadását követő napon lép hatályba, ezzel egyidejűleg a Borsod-Abaúj-Zemplén Vármegyei Katasztrófavédelmi Igazgatóság adatvédelmi, adatbiztonsági és közérdekű adatok nyilvánosságára vonatkozó szabályzatának kiadásáról szóló 25/2024. számú intézkedés hatályát veszti.

Macz János Zsolt tűzoltó ezredes
igazgató

JOGI SZEMPONTBÓL MEGFELELŐ
2025. 07. 10.

cep. 2025 JÚL 10.

Melléklet: 1. melléklet Adatvédelmi, adatbiztonsági és közérdekű adatok nyilvánosságára vonatkozó szabályzat

Készítette: dr. Polyák Zsolt tű. alezredes
Készült: 1 példányban
Kapják: 1.sz. példány: Irattár
Digitális formában: Szakterületi vezetők, KvK, HTP

1. melléklet a 25/2024. BAZ VMKI Igazgatói intézkedéshez

A Borsod-Abaúj-Zemplén Vármegyei Katasztrófavédelmi Igazgatóság adatvédelmi, adatbiztonsági és közérdekű adatok nyilvánosságára vonatkozó szabályzata

I. Fejezet

Általános rendelkezések

1. A szabályozás célja

1. A hivatásos katasztrófavédelmi szerv adatvédelmi, adatbiztonsági és közérdekű adatok nyilvánosságára vonatkozó szabályzata (a továbbiakban: Szabályzat) kibocsátásának célja, hogy a hivatásos katasztrófavédelmi szerv tevékenysége során a személyes adatok védelméhez fűződő alkotmányos alapjogon alapuló információs önrendelkezési jog érvényesülését biztosítsa, illetve az általa kezelt személyes adatok jogosulatlan felhasználásának megakadályozása érdekében meghatározásra kerüljenek az adatvédelmi és adatbiztonsági előírások, valamint a hivatásos katasztrófavédelmi szerv kezelésében lévő közérdekű adatok nyilvánosságának biztosítása, ennek érdekében a közérdekű adatok megismerésére irányuló igények elbírálása, illetve az elektronikus formában közzéteendő adatok megismerésére irányuló igények elbírálása során irányadó eljárási szabályok, valamint az elektronikus formában közzéteendő adatok nyilvánosságra hozatalával összefüggő feladatok meghatározása.

2. A hivatásos katasztrófavédelmi szerv adatkezelési tevékenységében állandó vagy eseti jelleggel részt vevő vagy abban közreműködő, a hivatásos katasztrófavédelmi szerv érdekkörében adatfeldolgozóként vagy közös adatkezelőként eljáró természetes és jogi személyekkel, jogi személyiséggel nem rendelkező szervezetekkel kötendő szerződésekben, megállapodásokban érvényesíteni kell a személyes adatok kezelésére vonatkozóan a Szabályzatban meghatározott követelményeket.

3. A Szabályzatban foglaltakat kell alkalmazni a hivatásos katasztrófavédelmi szerv által folytatott adatkezelési műveletekre az adatok megjelenési formájától függetlenül, az adatkezelés teljes folyamatára kiterjedően – az adatok megszerzésétől vagy a hivatásos katasztrófavédelmi szervnél történő keletkezésétől azok törléséig, illetve megsemmisítéséig –, függetlenül attól, hogy az adatok valamely nyilvántartási rendszer vagy valamely ügyben keletkezett irat részét képezik-e.

4. A minősített adatok kezelésére vonatkozó jogszabály eltérő rendelkezésének hiányában a Szabályzatban foglaltakat kell alkalmazni a minősített adathordozóban szerepeltetett személyes adatok kezelése során.

2. Értelmező rendelkezések

5. A Szabályzat alkalmazása során

5.1. *adatbiztonság*: a személyes adatok jogosulatlan kezelése, így különösen megszerzése, közlése, feldolgozása, megváltoztatása, elvesztése és megsemmisítése elleni szervezési, technikai megoldások, valamint eljárási szabályok összessége; az adatkezelés azon állapota, amelyben a kockázati tényezőket – és ezáltal a fenyegetettséget – a szervezési, műszaki megoldások és intézkedések megszüntetik, vagy legalább minimális szintre csökkentik;

5.2. *adatfelelős személy*: az adatfelelős szervezeti elemnél kijelölt személy, aki felelős a közzétételi listák részét képező adatok adatközlő felé történő továbbításáért;

5.3. *adatfelelős szervezeti elem*: a hivatásos katasztrófavédelmi szerveknél az a szervezeti elem, amely az elektronikus úton kötelezően közzéteendő közérdekű adatot előállította, illetve

amelynek a működése során ez az adat keletkezett, vagy amely részére működése során az adatot szolgáltatták;

5.4. *adathordozó*: bármely alakban, bármilyen eszköz felhasználásával és bármely eljárással előállított, személyes adatot tartalmazó, megjelenítő vagy azt megőrző tárgy, eszköz vagy közeg;

5.5. *adatkezelési tevékenységek nyilvántartása*: a hivatásos katasztrófavédelmi szerv felelősségi körébe tartozóan végzett, 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, 2016. április 27-i 2016/679 európai parlamenti és tanácsi rendelet hatálya alá tartozó adatkezelési tevékenységeket tartalmazó nyilvántartás, amelyet az adatvédelmi tisztviselő vezet;

5.6. *adatkezelői nyilvántartás*: a hivatásos katasztrófavédelmi szervek kezelésében lévő bűnügyi személyes adatokkal kapcsolatos adatkezeléseket tartalmazó nyilvántartás, amelyet az adatvédelmi tisztviselő vezet;

5.7. *adatközlő*: a hivatásos katasztrófavédelmi szervek azon szervezeti eleme vagy az a személy, amely, vagy aki az adatfelelős által hozzá eljuttatott adatokat a szerv közzétételi listáiban közzéteszi;

5.8. *adatvédelem*: a személyes adatok jogszerű kezelését, az érintett személyek védelmét biztosító alapelvek, szabályok, eljárások, adatkezelési eszközök és módszerek összessége

5.9. *közzétételi lista*: a hivatásos katasztrófavédelmi szervek által honlapjukon kötelezően nyilvánosságra hozott adattartalom, amely

a) *általános közzétételi lista*: az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) 37. § (1) bekezdése alapján, az Infotv. 1. mellékletében meghatározott adattartalommal rendelkező közzétételi lista;

b) *különös közzétételi lista*: az Infotv. 37. § (2) bekezdése alapján, jogszabály által a hivatásos katasztrófavédelmi szerveket is magában foglaló ágazatokra, a közfeladatot ellátó vagy rendvédelmi szervtípusra vonatkozóan meghatározott, közzéteendő adatokat tartalmazó közzétételi lista;

c) *egyedi közzétételi lista*: az Infotv. 37. § (3) bekezdése alapján a hivatásos katasztrófavédelmi szerv vezetője – a Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: NAIH) véleményének kikérésével –, valamint jogszabály által a hivatásos katasztrófavédelmi szervekre, azok irányítása, felügyelete alá tartozó szervekre vagy azok egy részére kiterjedő hatállyal kötelezően közzéteendő adatkört tartalmazó közzétételi lista.

II. Fejezet

A hivatásos katasztrófavédelmi szerv adatvédelmi intézményrendszere

3. Az adatkezelések szintjei

6. A hivatásos katasztrófavédelmi szerv központi adatkezelő szerve a Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóság (a továbbiakban: BM OKF), területi adatkezelő

szervek a katasztrófavédelmi igazgatóságok, a BM OKF Gazdasági Ellátó Központ (a továbbiakban: BM OKF GEK) és a Katasztrófavédelmi Oktatási Központ (a továbbiakban: KOK). A katasztrófavédelmi kirendeltségek és a hivatásos tűzoltóságok a katasztrófavédelmi igazgatóságok irányításával látnak el adatvédelmi feladatokat.

4. Az adatkezelő szerv vezetőjének felelősségi rendszere

7. Az adatvédelemre és információszabadságra vonatkozó előírások alkalmazása során adatkezelő szerv vezetőjének kell tekinteni a Borsod-Abaúj-Zemplén Vármegyei Katasztrófavédelmi Igazgatóságot (a továbbiakban: BAZ VMKI) igazgatóját.

8. Borsod-Abaúj-Zemplén VMKI igazgatója felelős

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

b) a kezelésében lévő közérdekű adatok közzétételi kötelezettségének teljesítéséért;

c) a közérdekű és a közérdekből nyilvános adatok kiadására irányuló adatigénylések határidőben történő megválaszolásáért;

d) a közzétételi egységek leíró adatainak az egységes közadatkereső rendszer üzemeltetőjéhez történő továbbításáért és a továbbított adatok rendszeres frissítéséért;

e) az alárendelt személyi állomány adatvédelmi oktatásáért és továbbképzéséért;

f) az irányítása alá tartozó szerv tevékenységének rendszeres adatvédelmi ellenőrzéséért, az ellenőrzés során esetlegesen feltárt hiányosságok vagy jogszabálysértő körülmények megszüntetéséért, a személyi felelősség megállapításához szükséges eljárás kezdeményezéséért, illetve lefolytatásáért, az általa vezetett szerv közzétételi listáinak naprakészségéért;

g) az érintett jogainak gyakorolásához szükséges feltételek biztosításáért.

9. Az adatkezelő szervek vezetőinek felelőssége nem zárja ki az egyes szervezeti elemek, valamint az egyes állománytagok felelősségét.

10. Amennyiben a személyes adatokhoz való jog megsértése miatt a hivatásos katasztrófavédelmi szervnek sérelemdíj, kártérítés fizetési kötelezettsége keletkezik, a személyes adatokhoz fűződő jogsértést ténylegesen elkövető személy kilétének felderítésére mindent meg kell tenni, és amennyiben ez sikerrel jár, vele szemben kártérítési eljárást kell kezdeményezni.

5. A BAZ VMKI igazgatójának feladat- és hatásköre

11. A BAZ VMKI igazgatójának feladat- és hatásköre:

a) kialakítja és irányítja a jogszabály által a feladat- és hatáskörbe utalt adatkezelési rendszerek egészének (nyilvántartások, adattárak, munkafolyamatok, információáramlások és feldolgozások, jogosultságok), rendeltetésszerű működtetését, amelynek keretében teljes felelősséget visel a személyes adatok kezeléséért, valamint az információszabadságra vonatkozó jogszabályok és az ezen alapuló rendelkezések érvényre juttatásáért;

b) gondoskodik a személyes adatok körében a jogosulatlan hozzáférés, közlés, megváltoztatás, vagy törlés megelőzéséről, a szervezési-, technikai védelemről, továbbá, 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, adathordozhatósághoz való jogát, kérésére az adatkezelő korlátozza az adatkezelést, amennyiben annak feltételi fennállnak, tiltakozhasson személyes adatai kezelése ellen;

c) személyes felelősséggel tartozik az általa vezetett szerv, illetve az 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 minősítettadat-védelmi szabályok betartásáért;

d) ellenőrzi a védelmi és biztonsági szabályok gyakorlati érvényesülését, intézkedik a hiányosságok felszámolására;

e) kialakítja az adatkezelések szervezeti és működési feltételeit, gondoskodik a működési követelmények és az adatbiztonsági követelmények érvényre juttatásáról.

6. A BAZ VMKI adatvédelmi tisztviselője

12. A BAZ VMKI igazgatója köteles az irányítása alá tartozó személyi állományból az adatvédelmi tevékenység, támogatása, felügyelete és ellenőrzése érdekében – jogi, közigazgatási, informatikai felsőfokú végzettséggel rendelkező – területi adatvédelmi tisztviselőt kijelölni. A BAZ VMKI adatvédelmi tisztviselője az adatkezelő szervnél más feladatokat is elláthat, azonban az adatkezelő szerv vezetője köteles biztosítani, hogy ezekből a feladatokból adódóan ne keletkezzen összeférhetetlenség, és az egyéb munkaköri feladatok ellátása ne veszélyeztesse az adatvédelmi tisztviselői feladatok ellátását. Az összeférhetetlenség fennállását folyamatosan vizsgálni kell.

13. A BAZ VMKI adatvédelmi tisztviselője eljár a munkaköri leírásában rögzített adatvédelemmel összefüggő feladatkörökben, az adatkezelő szerv vezetője ugyanakkor továbbra is felelős az adatkezelés jogszerűsége érdekében hatáskörébe tartozó intézkedések megtételéért. A területi adatvédelmi tisztviselő adatvédelmi feladatainak gyakorlása során az őt kinevező vezető közvetlen alárendeltségébe tartozik.

14. A BAZ VMKI adatvédelmi tisztviselője köteles jelenteni az adatkezelő szerv vezetőjének, amennyiben azt észleli, hogy egy ügy elintézése kapcsán vele kapcsolatban összeférhetetlenségi helyzet merül fel, így különösen, ha az alapul szolgáló üggyel összefüggő adatkezelési tevékenység kapcsán korábban döntést hozott. Ebben az esetben az ügy elintézésével kapcsolatos döntési jogkört az adatkezelő szerv vezetője gyakorolja, aki a döntés előkészítésére kijelöli az ügyben eljáró szervezeti egységet.

15. A BAZ VMKI adatvédelmi tisztviselőjének feladata:

a) segíti az adatkezelő szerv vezetőjét az adatkezelésre vonatkozó jogszabályok és belső normák érvényre juttatásában, figyelemmel kíséri az adatvédelemmel összefüggő jogszabályváltozásokat, előkészíti az adatkezelő szerv vezetőjének adatvédelmi tárgyú döntéseit;

b) kivizsgálja a hozzá érkezett bejelentéseket; és adatvédelmi incidens észlelése esetén annak megszüntetésére hívja fel az adatkezelőt vagy az adatfeldolgozót, indokolt esetben vizsgálat lefolytatását kezdeményezi az adatkezelő szerv vezetőjénél, javaslatot tesz az incidens káros következményeinek elhárítására, a hasonló jövőbeni incidensek megelőzésére;

c) segítséget nyújt az érintettek jogainak gyakorlásában;

d) az adatkezelő szerv vezetőjének megbízásából ellenőrzi az adatkezelő szervnél, illetve az alárendelt 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;

e) gondoskodik a területi szerv személyi állománya és a helyi adatvédelmi megbízott oktatásáról, szükség szerinti vizsgáztatásáról, a helyi szerv személyi állományának oktatásához segédanyagot biztosít a részére vagy az oktatást ő maga végzi;

f) elkészíti az adatkezelő szerv adatvédelmet érintő belső normáinak tervezetét, közreműködik az adatvédelmi jogszabályok és magasabb szintű belső normák tervezeteinek véleményezésében, jelzi a jogalkalmazás során tudomására jutott, esetleges normamódosítást igénylő problémákat;

g) vezeti az adatkezelői tevékenységek nyilvántartását, az adatkezelői nyilvántartás, az adatvédelmi incidensek nyilvántartását, az érintett hozzáférési jogával kapcsolatos intézkedésekről szóló nyilvántartást és az elutasított közérdekű adat megismerési kérelmek nyilvántartását;

h) a kérelem tárgyában érintett szakterület közreműködésével elkészíti az érintettnek a személyes adatai kezelésére vonatkozó kérelmére, illetve a közérdekű adat megismerésére irányuló kérelmekre adandó válasziratokat;

i) gondoskodik a területi adatkezelő szerv honlapján megjelenített Adatvédelmi Irányelvek és adatkezelési tájékoztatók naprakészen tartásáról;

j) rendszeresen ellenőrzi a területi adatkezelő szerv közzétételi listáinak naprakészségét és teljességét, az egyes szakterületeket adatközlésre hívja fel;

k) felügyeli az adatkezelő szerv adatszolgáltatási tevékenységét, adatvédelmi szempontból állást foglal az adatok továbbításának jogszerűségével kapcsolatban;

l) feladatának ellátása során szükség szerint együttműködik a rendszergazdával, illetve – amennyiben van ilyen – az elektronikus információs rendszerek biztonságáért felelős személlyel;

m) évente január 20-ig jelentésben értékeli a területi és helyi szerv adatvédelmi, adatbiztonsági és információszabadsággal kapcsolatos helyzetét;

n) végzi az elutasított közérdekűadat-megismerési igényekkel kapcsolatos NAIH felé teljesítendő tájékoztatást;

o) ellátja az Egységes Közadatkereső Rendszerrel, a Központi Jegyzékkel, valamint a Központi Információs Közadat-nyilvántartással kapcsolatos, jogszabályban meghatározott feladatokat;

p) közreműködik az adatvédelmi tárgyú perben, szakmai véleményével segíti a BAZ VMKI kijelölt jogtanácsosának perképviseletét, a tárgyalásokon hallgatóságként részt vesz;

q) segíti az adatvédelmi hatásvizsgálatot, közreműködik az adatfeldolgozói, közös adatkezelői szerződések megkötésében;

r) ellátja mindazon feladatokat, amelyeket a területi adatkezelő szerv Adatvédelmi és Adatbiztonsági Szabályzata részére feladatként meghatároz.

16. A 15. pont m) alpontjában 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 elvégzett honlap ellenőrzések időpontját, eredményét és a hiányosságok pótlására vonatkozó információkat;

c) az adatkezelő szervek állományába tartozók ellen az adatvédelmi előírások megsértése miatt indított fegyelmi, szabálysértési és büntetőeljárásokra vonatkozó adatokat (az érintettek megjelölése nélkül);

d) az adatkezelő szerveknél lefolytatott oktatások, továbbképzések gyakorlatát;

e) a NAIH által végzett vizsgálatokat, megkereséseket, azok fontosabb megállapításait;

f) adatvédelemmel, információszabadsággal kapcsolatos perekre vonatkozó adatokat;

g) a közérdekű adatok nyilvánosságának egyedi kérelmek útján és honlapon történő közzététellel biztosított helyzetét az adatkezelő szervnél, ideértve NAIH részére az Infotv. alapján készített éves jelentés adatlapját,külön kitérve az egy témakörben beérkezett több adatigényre;

h) az adatvédelem és információszabadság területén adódott egyedi ügyeket;

i) a következő naptári évre tervezett feladatokat.

7. A BAZ VMKI kirendeltségeinek adatvédelmi megbízottai

17. A BAZ VMKI vezetője az ellátandó feladatok jellege, összetettsége és mennyisége alapján a BAZ VMKI adatvédelmi tisztviselő tevékenységének támogatása érdekében a kirendeltség állományából adatvédelmi megbízottat jelölhet ki.

18. A helyi adatvédelmi megbízottak közreműködnek a személyes adatok jogszerű kezelését biztosító feladatok végrehajtásában. Az adatvédelmi megbízott a helyi szerv adatvédelmi követelményeknek megfelelő működésének biztosítása érdekében közreműködik az adatvédelmi tisztviselő által meghatározott feladatok ellátásában.

19. Az adatvédelmi tisztviselő az adatvédelmi megbízott számára a Szabályzatban meghatározott tevékenységében történő közreműködés érdekében feladatot határozhat meg.

20. A helyi adatvédelmi megbízott eljár a részére meghatározott – és munkaköri leírásában rögzített – adatvédelemmel összefüggő feladatkörökben, a területi adatkezelő szerv vezetője

ugyanakkor továbbra is felelős az adatkezelés jogszerűsége érdekében hatáskörébe tartozó intézkedések megtételéért.

21. A BAZ VMKI adatvédelmi megbízottainak feladata:

a) közreműködik a helyi adatkezelő szerv adatkezelésével összefüggésben érkező panaszok, kifogások kivizsgálásában,

b) segítséget nyújt az érintetteknek a helyi adatkezelő szerv adatkezelésével összefüggésben, jogaik gyakorlásához,

c) a katasztrófavédelmi kirendeltség vezetőjének megbízásából ellenőrzi a helyi adatkezelő szervnél vagy annak egységeinél (tűzoltó-parancsnokság) az adatvédelmi követelmények megtartását, az előírások megszegésének észlelése esetén felhív a jogszerű állapot haladéktalan helyreállítására és a hiányosságokat a szolgálati út betartásával jelzi a szerv vezetőjének és indokolt esetben a szerv vezetőjénél kezdeményezi a felelősség megállapításához szükséges eljárás lefolytatását,

d) a c) ponton felül, havonta ellenőrzi a fizikai adatbiztonságra vonatkozó szabályok betartását,

e) közreműködik az adatvédelmi jogszabályok és magasabb szintű belső normák tervezeteinek véleményezésében, jelzi a jogalkalmazás során tudomására jutott, normamódosítást igénylő problémákat,

f) állásfoglalás kialakításával, véleményezéssel segíti a helyi adatkezelő szerv adatvédelmet érintő szakmai tevékenységét,

g) évente február 15. napjáig – a részére előzetesen megküldött szempontrendszer alapján – jelentésben értékeli a helyi adatkezelő szerv adatvédelmi és adatbiztonsági helyzetét.

8. A területi adatvédelmi tisztviselőre és a helyi adatvédelmi megbízottra vonatkozó közös szabályok

22. Az adatvédelmi tisztviselőt és az adatvédelmi megbízottat a személyes adatok védelme területén szerzett ismeretei és gyakorlati tapasztalatai, valamint a számára jogszabályban vagy normában meghatározott feladatok ellátására munkaköréből, ismereteiből adódó alkalmasság alapján, írásban kell kijelölni.

23. Nem lehet olyan személyt kijelölni adatvédelmi tisztviselőnek vagy adatvédelmi megbízottnak, akinek a Polgári Törvénykönyvről szóló 2013. évi V. törvény szerinti hozzátartozója az adatkezelő szervnél adatkezeléssel kapcsolatos döntések meghozatalára jogosult személy.

24. Az adatvédelmi tisztviselő és az adatvédelmi megbízott munkaköri leírásának tartalmaznia kell a főbb ellátandó feladatait, különösen azt, hogy tevékenységét mely szervek vonatkozásában végzi.

25 Az adatvédelmi tisztviselő számára feladatainak ellátása céljából, az ahhoz szükséges mértékben biztosítani kell a minősítéssel védett iratokba történő betekintést.

26. Adatvédelmi tisztviselőnek és adatvédelmi megbízottnak felsőfokú végzettséggel rendelkező és az adatvédelmi ismeretekből sikeres vizsgát tett személy jelölhető ki. Az

adatvédelmi tisztviselő a BM OKF adatvédelmi tisztviselője által szervezett képzést követő vizsga teljesítésével igazolja a szükséges adatvédelmi ismeretek meglétét.

III. Fejezet

A személyes adatok védelme a hivatásos katasztrófavédelmi szervnél

9. Az adatkezelés alapvető szabályai

27. A BAZ VMKI-nál kezelt 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.

28. Az adatkezelő köteles az adatkezelési műveleteket úgy megtervezni és végrehajtani, hogy biztosítsa az érintettek magánszférájának védelmét.

29. 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.

30. 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.

31. Az adatkezelőnek és az adatfeldolgozónak az adatok biztonságát szolgáló intézkedések meghatározásakor és alkalmazásakor tekintettel kell lenni a technika mindenkori fejlettségére, és a rendelkezésre álló legjobb technológiát az érintettek magánszférájának védelme érdekében alkalmazni kell. Több lehetséges adatkezelési megoldás közül azt kell választani, amely a személyes adatok magasabb szintű védelmét biztosítja, kivéve, ha az aránytalan nehézséget jelentene az adatkezelőnek.

32. A közfoglalkoztatottak kizárólag abban az esetben láthatnak el ügykezelői, ügyviteli feladatokat, amennyiben a munkavégzés céljából rendelkezésükre bocsátott adatok kezelése egyértelműen azonosítható és esetleges későbbi adatsértés esetén bizonyítható, hogy ki és milyen mértékben ismerhette meg azokat, valamint a jelen szabályzatban, a Hivatásos Katasztrófavédelmi Szervek Egységes Iratkezelési Szabályzatában és az Informatikai Biztonsági Szabályzatban foglaltak ismeretéből az adatvédelmi tisztviselő és az ügykezelésért felelős vezető által szervezett oktatáson eredményes vizsgát tett, továbbá, amennyiben a közfoglalkoztatott nyilatkozatot tesz, amelyben felelősséget vállal az adatvédelmi és adatbiztonsági szabályok betartásáért. A közfoglalkoztatottak feladataik ellátása során kizárólag az ügyviteli tevékenységhez kapcsolódó adatfeldolgozási tevékenységben történő részvétel tekintetében kerülhetnek kapcsolatba a hivatásos katasztrófavédelmi szerv állományába tartozó személyre vonatkozó személyes vagy különleges adattal, megjelenési formájától függetlenül, humánigazgatási eljárást érintő iratanyagot, illetve az illetményre, juttatásokra vonatkozó iratokat, adatokat, nyilvántartásokat nem kezelhetnek. Ezen adatokat még az ügyviteli tevékenységhez kapcsolódó adatfeldolgozási tevékenységben történő részvétel tekintetében sem kezelhetik.

10. Adatkezelések megkezdése, adatvédelmi hatásvizsgálat, az érintetti jogok

33. Amennyiben a személyesadat-kezelés belső szabályozó vagy egyéb írásos formában kerül elrendelésre, erre országos szinten a BM OKF főigazgatója vagy a szakterület szerint érintett helyettese, területi szintű adatkezelés esetén az érintett területi szerv vezetője jogosult.

34. Személyesadat-kezelési kötelezettséget előíró belső szabályozó vagy írásbeli döntés előkészítése során az érintett szakterület, ha a tervezett adatkezelés valamely – különösen új technológiákat alkalmazó – típusa magas kockázattal jár a természetes személyek jogaira és szabadságára nézve, vagy ha az adatkezelés a NAIH hatásvizsgálati jegyzékében szerepel, előzetes hatásvizsgálatot végez arra vonatkozóan, hogy a tervezett adatkezelési műveletek a személyes adatok és az érintettek védelmét hogyan érintik.

35. Nem kell adatvédelmi hatásvizsgálatot végezni, ha az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges vagy közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges, és az adatkezelést jogszabály írja elő, amennyiben a jogalkotó a jogszabály-előkészítés során adatvédelmi hatásvizsgálatot végzett.

36. Az adatvédelmi hatásvizsgálat szükségességének megállapításához az érintett szakterület megválaszolja az 1. függelékben foglalt kérdéseket.

37. Ha a tervezett adatkezelés annak körülményeire, így különösen céljára, az érintettek körére, az adatkezelési műveletek során alkalmazott technológiára tekintettel – az adatkezeléssel várhatóan érintett személyek jogaira és szabadságaira nézve – valószínűsíthetően magas kockázatot nem azonosít, vagy megállapítást nyer, hogy az adatkezelés az adatvédelmi jogszabályban meghatározott kivételi körbe tartozik, úgy ennek tényét az érintett szakterület írásban rögzíti.

38. Amennyiben az érintett szakterület az adatkezeléssel várhatóan érintett személyek jogaira és szabadságaira nézve magas kockázatot azonosít vagy jogszabályi rendelkezés alapján adatvédelmi hatásvizsgálattal kötelezően vizsgálandó adatkezelési tevékenységek esete áll fenn, adatvédelmi hatásvizsgálat lefolytatását kezdeményezi az adatkezelő szerv vezetőjénél.

39. Az adatkezelő szerv vezetője az érintett szakterület javaslatára elrendeli az adatvédelmi hatásvizsgálat lefolytatását vagy írásban rögzíti mellőzésének okait. Az adatvédelmi hatásvizsgálat lefolytatásáig vagy az annak elmaradásával kapcsolatos okok írásban történő rögzítéséig az adatkezelésről szóló döntés nem hozható meg.

40. Az adatvédelmi hatásvizsgálat lefolytatásában az adatkezelés által érintett szakterület vesz részt. Az adatvédelmi hatásvizsgálatot az adatvédelmi tisztviselő és az elektronikus információs rendszer biztonságáért felelős személy segíti. Az adatvédelmi hatásvizsgálat iratai döntés-előkészítő iratok, ezért azok nem nyilvánosak.

41. Az adatkezelési hatásvizsgálatot végző szakterület az adatvédelmi hatásvizsgálatról összefoglaló jelentést készít a 2. függelékben foglaltak alapján. Az összefoglaló jelentést az adatkezelő szerv vezetője hagyja jóvá, amelyet követően az adatkezelést a 34. pont szerint kell elrendelni.

42. Az érintett hozzájárulásán alapuló adatkezelés esetén – későbbi igazolhatósága érdekében – a hozzájárulást különleges adatnak nem minősülő személyes adatok esetén is írásban kell rögzíteni, kivéve a 106. pontban foglalt esetben.

43. 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 (előzetes tájékozódáshoz, hozzáféréshez, helyesbítéshez, az adatkezelés korlátozásához, törléshez, adathordozhatósághoz való jog) és azokat milyen módon érvényesítheti;

e) az adatok esetleges automatizált döntéshozatal céljából való felhasználásáról;

f) a hozzájárulás bármely időpontban történő visszavonásának jogáról és arról, hogy a hozzájárulás visszavonása nem érinti a visszavonást megelőző adatkezelés jogszerűségét;

g) 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;

h) az adatvédelmi tisztviselő elérhetőségéről;

i) milyen jogorvoslati lehetőséggel rendelkezik (NAIH-hoz fordulás, bírósági jogérvényesítés útja).

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

45. Az egyedi ügyekben alkalmazandó hozzájáruló nyilatkozatot, valamint az ahhoz tartozó adatvédelmi tájékoztatót az adatkezelő szerv adatvédelmi tisztviselője, a rendszeresen előforduló, adatkezelési hozzájárulást igénylő ügyekben alkalmazandó hozzájáruló nyilatkozatot a BM OKF adatvédelmi tisztviselője az érintett szakterület közreműködésével készíti el.

46. A több hivatásos katasztrófavédelmi szerv által ugyanazon adatokon végzett adatkezelés esetén az adatkezelésről történő tájékoztatás és a hozzájáruló nyilatkozat elkészítése során ügyelni kell arra, hogy valamennyi adatkezelő szerv adatkezelőként történő megjelölésére sor kerüljön.

47. Egy adatállományhoz több adatkezelési cél is kapcsolódhat, azonban minden egyes célhoz rendelkezésre kell állnia a szükséges jogalapnak.

11. Adatvédelmi incidensek nyilvántartása

48. Aki a tevékenységének ellátása során a hivatásos katasztrófavédelmi szerv által végzett adatkezeléssel kapcsolatban adatvédelmi incidens gyanúját észleli, köteles azt a szolgálati út betartásával a vonatkozó belső szabályozó szerint haladéktalanul jelezni a hivatásos katasztrófavédelmi szerv adatvédelmi tisztviselőjének.

49. Aki a munkáltató által végzett adatkezelés kapcsán saját személyes adatai tekintetében adatvédelmi incidens gyanúját észleli, jogosult azt közvetlenül jelezni a BAZ VMKI adatvédelmi tisztviselőjének.

50. Az adatvédelmi tisztviselő az 49–50. pont alapján neki bejelentett és a saját hatáskörben észlelt adatvédelmi incidensekről 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.

51. A bekövetkezett adatvédelmi incidensek tekintetében a következmények elhárítási és a hasonló esetek bekövetkezésének megelőzési módjára az adatvédelmi tisztviselő tesz javaslatot.

12. Az adatkezelési tevékenységek nyilvántartása

52. Az adatvédelmi tisztviselő legkésőbb az adatkezelés megkezdése előtti tizennegyedik napig köteles az adatkezelő hivatásos katasztrófavédelmi szerv felelősségébe tartozóan kezelt személyes adatokkal kapcsolatos adatkezelésekről vezetett nyilvántartásban rögzíteni a személyes adat érintettjének 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, 2016. április 27-i 2016/679 európai parlamenti és tanácsi rendelet (a továbbiakban: GDPR) 30. cikk (1) bekezdésében foglaltakat.

53. Az adatkezelésekben bekövetkezett változást vagy az adatkezelés megszüntetését az érintett szakterület nyolc napon belül bejelenti az adatvédelmi tisztviselőnek.

13. Az adatkezelői nyilvántartás

54. A hivatásos katasztrófavédelmi szerv a kezelésében lévő bűnüldözési célú adatkezelés (katonai vétség miatti parancsnoki nyomozás) esetén adatkezelői nyilvántartásban rögzíti az Infotv. 25/E. § (1) bekezdésében foglaltakat.

14. Az adatfeldolgozás szabályai

55. Az adatfeldolgozásra vonatkozó szerződést vagy más jogi aktust írásba kell foglalni, amely a GDPR 28. cikk (3) bekezdésében foglaltakon túl a tartalmazza különösen

a) az adatkezelő és az adatfeldolgozó megnevezését,

b) az adatfeldolgozói feladatot képező technikai műveletek pontos meghatározását,

c) a feldolgozásra átadott adatbázis vagy adatkör megjelölését,

d) az átadott személyes adatok tárolására és megőrzésére vonatkozó rendelkezéseket,

e) a szerződés teljesítése, megszűnése esetére – így különösen az eredeti és a feldolgozott adatbázis visszaszolgáltatására, törlésére, e műveletek jegyzőkönyvezésére – vonatkozó rendelkezéseket,

f) a felelősségi kérdéseket,

g) a további adatfeldolgozó igénybevételének lehetőségét vagy tilalmát,

h) az adatfeldolgozó kötelezettségét, hogy az adatkezelő írásbeli utasítása szerint jár el,

i) az adatfeldolgozónál személyes adatokhoz való hozzáférésre feljogosított személyek titoktartási kötelezettségét és

j) az adatkezelő részére nyújtott, az érintettek jogainak érvényesítésében való segítségnyújtási és az adatkezelő részére történő információátadási kötelezettséget.

15. Közös adatkezelés szabályai

56. Amennyiben ugyanazon személyes adatok kezelésének céljait és eszközét két vagy több hivatásos katasztrófavédelmi szerv vagy hivatásos katasztrófavédelmi szerv és más szerv közösen határozza meg, az adatkezelés szabályait megállapodásban rögzítik, kivéve, ha az adatvédelmi jogszabályok szerinti kötelezettségeik teljesítéséért fennálló, feladataikkal összefüggő felelősségük megosztását jogszabály határozza meg.

16. Adattovábbítás a hivatásos katasztrófavédelmi szervek adatkezeléseiből

57. A hivatásos katasztrófavédelmi szerv adatkezeléseiből adatvédelmi szempontból akkor tekinthető az adattovábbítás jogszerűnek, ha a személyes adat birtokában lévő szerv vagy személy jogosult annak továbbítására, az adattovábbítás címzettje (adatkérő) rendelkezik az adat kezeléséhez szükséges jogalappal, harmadik országba vagy nemzetközi szervezet részére történő adattovábbítás esetén a GDPR V. fejezetében foglalt valamely garanciával vagy az érintett – a vonatkozó jogszabályi elvárásoknak megfelelő tartalmú – írásos hozzájárulásával, és az adatkérés célja mindezzel összhangban van.

58. Az adattovábbítás feltételeinek meglétét az adatot továbbító adatkezelő minden egyes személyes adattal összefüggésben ellenőrizni köteles.

59. Harmadik személy vagy szerv által benyújtott adattovábbítási kérelem elbírálása – a törvényben kötelezően előírt adattovábbítás esetét kivéve – az adatkezelő szerv vezetőjének, vagy az általa kijelölt vezetőnek a hatáskörébe tartozik. Az adatigénylést abban az esetben teljesítheti, ha az tartalmazza

a) az adatigénylés célját, jogalapját;

b) a kért adatok körének pontos meghatározását;

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

60. A hivatásos katasztrófavédelmi szerv – törvény eltérő rendelkezése hiányában – csak olyan személyes adatokat továbbíthat, amelyeknek a hivatásos katasztrófavédelmi szerv az adatkezelője. Azokban az esetekben, amikor az adatigénylés olyan személyes adatra vonatkozik, amely esetében a törvényben meghatározott adatkezelő más szerv, az adatkérést –

törvény eltérő rendelkezése hiányában – el kell utasítani és az adatkérőt tájékoztatni kell arról, hogy a kért adatokat mely szervtől igényelheti.

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

62. A személyes adatnak nem minősülő adatok továbbítása során is kiemelt figyelmet kell fordítani arra, hogy az adat továbbításának jogszabályban meghatározott korlátja fennáll-e. Szükség esetén ki kell kérni az adatvédelmi tisztviselő véleményét.

17. A közvetlen lekérdezés

63. A közvetlen lekérdezés lehetőségének megteremtésére irányuló kérelmet az adatkezelő szerv vezetője – az érintett szakmai szakterület és az informatikai rendszerek biztonságáért felelős előzetes javaslata alapján – bírálja el. Amennyiben a szükséges biztonsági feltételek nem állnak fenn, vagy azok megteremtését és fenntartását a kérelmező nem vállalja, a közvetlen hozzáférés nem biztosítható.

64. A közvetlen hozzáférés feltételeinek fennállása esetén az adatkezelő és az adatigénylő megállapodást – nem a Belügyminisztérium irányítása alá tartozó szerv esetén szerződést – köt a rendszer igénybevételének feltételeiről, illetve a rendszer használatának technikai és adatbiztonsági követelményeiről, valamint a költségviselés rendjéről.

65. A megállapodás, illetve a szerződés alapján kiadott közvetlen lekérdezési engedély tartalmazza a lekérdezések célját, jogalapját, a lehívható adatfajtákat, a lekérdezésre feljogosított személyi kör megjelölését, a lekérdezési lehetőség kezdő és végső időpontját, valamint az adatok jogszerű felhasználására felhívó záradékot.

66. A lekérdezési lehetőség biztosítása esetén a lekérdezett adatokhoz csak az arra jogosultak férhetnek hozzá. A közvetlen lekérdezést biztosító rendszerből kizárólag az engedélyezett célra és az engedélyben meghatározott adatok kérhetők le, valamint a lekérdezett adatokat csak jogszerű – az engedélyben meghatározott – célra használhatók fel.

67. A lekérdezésre jogosult személyekről és egyedi azonosítójukról naprakész nyilvántartást kell vezetni. A jogosultak személyéről és az abban bekövetkezett változásokról az adatkezelő szervet kérésére – illetve a megállapodásban vagy a szerződésben meghatározott esetekben – tájékoztatást kell nyújtani.

68. A közvetlen lekérdezést biztosító rendszert úgy kell kialakítani, hogy a személyes adatokhoz történő hozzáférés egyedi azonosító és jelszó megadásához kötötten történjen és a lekérdezés naplózására sor kerüljön. A visszaélések megakadályozása érdekében a jelszavak kezelésének biztonságáról gondoskodni kell.

69. Az adatfelhasználás és a lekérdezés jogszerűségének dokumentálása érdekében a közvetlen lekérdezést biztosító rendszert úgy kell kialakítani, hogy a lekérdezést végző a lekérdezéskor a rendszer erre a célra kialakított állományában rögzíteni tudja az adatlekérdezés céljára utaló adatot (például az ügyszámot), amennyiben erre programtechnikailag nincs lehetőség az érintett adatkezelés megjelölését, az adatlekérdezés időpontját és célját dokumentálni kell.

18. Adattovábbítás hírközlő eszköz alkalmazásával

70. A hivatásos katasztrófavédelmi szervek által kezelt személyes adatot hírközlő eszközön csak a jogosult nyomozó hatóságok, nemzetbiztonsági szervek, bíróságok, valamint az adatkezelővel közös szervezetbe tartozó személyek számára, szervezetszerűen működő ügyfélszolgálat, ügyeleti szolgálat, illetve a Szervezeti és Működési Szabályzatában erre kijelölt szervezeti elem továbbíthat. Ettől eltérni csak halaszthatatlan esetben, az élet, a testi épség, az egészség vagy a vagyonbiztonság megóvása érdekében lehet.

71. A hívó jogosultságáról jelszó alkalmazásával, visszahívással vagy egyéb arra alkalmas módon meg kell győződni. Ha a hívó jogosultsága nem állapítható meg, a tájékoztatás hírközlő eszközön nem teljesíthető.

72. Abban az esetben, ha egy nyilvántartásból hordozható számítástechnikai eszközzel történik a lekérdezés és ezek naplózására az igénybe vett nyilvántartás nem alkalmas, akkor az adatlekérés időpontját, az adatkérő személyét (név, rendfokozat és beosztás megjelölésével), a kért adat fajtáját manuális módon kell rögzíteni és a hordozható számítástechnikai eszköz leadásakor azt az eszközt kezelő szervnek kell leadni.

73. Hírközlő eszközön történő adatszolgáltatás esetén a legszükségesebb adatok közlésére kell szorítkozni.

19. Az adatigénylés során irányadó szabályok

74. A hivatásos katasztrófavédelmi szervek adatállományaiból kizárólag a katasztrófavédelmi feladat- és hatáskörök gyakorlása érdekében, továbbá törvényben meghatározott esetben – a célhoz kötöttség elvének szigorú érvényre juttatása mellett – igényelhető és használható fel közérdekből nyilvánosnak nem minősülő személyes adat. A más adatkezelők által kezelt olyan adatállományokból, amelyekből történő adatigénylésre a hivatásos katasztrófavédelmi szerveket az érintett adatkezelésre irányadó törvény felhatalmazza, csak az adott törvényben meghatározott katasztrófavédelmi feladat ellátása érdekében végezhető adatlekérdezés, azok harmadik személynek vagy szervnek nem továbbíthatók.

75. Az egyes eljárások során a különböző adattárakból lekért, de az ügy szempontjából érdektelenné vált, fel nem használt személyes adatokat az ügy előadója az ügyirat továbbítását, illetve irattárba helyezését megelőzően köteles megsemmisíteni. A megsemmisítés tényét és időpontját az iratborítón, az előadói íven vagy az ügyiratban elhelyezett külön iraton rögzíteni és aláírással igazolni kell.

76. Az adatlekérdezés, illetve a megsemmisítéssel érintett adatok későbbi azonosíthatósága érdekében a lekérdezés időpontját, az érintett személy nevét és az igénybe vett nyilvántartás megjelölését kell rögzíteni, maguk a lekérdezett személyes adatok nem szerepeltethetők.

77. Az adatkérés naplózására irányadó szabályokat megfelelően alkalmazni kell az állomány részére az ügyeleti szolgálat által teljesített adatszolgáltatás esetén is. Ebben az esetben – a rendelkezésre álló technikai lehetőségek figyelembevételével számítógépen, hangrögzítéssel vagy manuális módon – rögzíteni kell az adatkérés időpontját, az adatkérő személyét (név, rendfokozat és beosztás megjelölésével), a kért adatok fajtáját és az adatszolgáltatást teljesítő személyét. A manuális naplózást az adatkérés kezdeményezője a szolgálat befejezését követően aláírásával hitelesíti, amennyiben erre nincs lehetőség, akkor a saját maga által vezetett nyilvántartásban dokumentálja az általa kezdeményezett lekérdezést.

78. A folyamatos ügyeleti szolgálatot ellátók esetében a nyilvántartásokba történő belépés és azokból adatszolgáltatás csak az ügyeleti szolgálatot ellátó személy saját hozzáférési kódjának felhasználásával történhet. A szolgálat átadásával egy időben ezért kötelesek kilépni a számítógépes rendszerekből, a szolgálatba lépők pedig saját jogosultságuk és azonosító kódjuk alapján belépni a rendszerekbe.

20. Az érintetti jogok gyakorlása

79. Az érintetti jogok gyakorlásának lehetőségére és módjára, a kapcsolattartó személyére és elérhetőségeire az érintettek figyelmét az adatkezelésre vonatkozó tájékoztatás nyújtása során a tájékoztató részeként fel kell hívni.

80. A hivatásos katasztrófavédelmi szerveknél az érintetti jogok gyakorlása tekintetében az érintettekkel az adatvédelmi tisztviselő tartja a kapcsolatot, kivéve, ha az adott jog és az adott adatkezelés tekintetében a szakterülettel történő közvetlen kapcsolattartás indokolt.

81. A beérkezett kérelmeket az adatvédelmi tisztviselő továbbítja az adatkezelést végző szervezeti elem részére.

82. Az érintettet megillető jogok gyakorlására csak az érintett kérelmező megfelelő azonosítása esetén van lehetőség.

83. Nem biztosítható ezen jogok gyakorlása különösen az elektronikus aláírással nem hitelesített, vagy a kérelmező személyének azonosítását nem biztosító úton érkezett kérelmek esetén. A biztonságos elektronikus kézbesítési szolgáltatás útján küldött kérelmet úgy kell tekinteni, hogy az a jogosulttól származik.

84. A beérkezett kérelmeket az adatkezelő indokolatlan késedelem nélkül, de legkésőbb a kérelem beérkezésétől számított egy hónapon belül, a megadott elérhetőségre küldött levélben teljesíti. Szükség esetén, figyelembe véve a kérelem összetettségét és a kérelmek számát, a határidő további két hónappal meghosszabbítható.

85. Amennyiben az érintett személyes adatának helyesbítését vagy törlését kéri, az adatot a kijavításig vagy a törlésig jelzéssel kell ellátni. Az adaton a tároláson túl egyéb adatkezelési műveletet kizárólag az érintett jogos érdekének érvényesítése céljából vagy törvényben meghatározottak szerint lehet végezni.

86. Az adat helyesbítéséről, törléséről és korlátozásáról az érintettet és mindazokat tájékoztatni kell, akiknek az adatot továbbították, kivéve, ha a tájékoztatás elmaradása az adatkezelés céljára tekintettel az érintett jogos érdekeit nem sérti. Ezen tájékoztatást a szervezeti elemek közvetlenül végzik, az adatvédelmi tisztviselőt a levél másolatának megküldésével tájékoztatják.

87. Az érintett hozzáférési jogának gyakorlása során az adatkezelő az érintett jogainak ismételt és megalapozatlan érvényesítésével összefüggésben közvetlenül felmerült költségeinek megtérítését a hivatásos katasztrófavédelmi szervekhez érkezett közérdekűadat-megismerési igények teljesítésével kapcsolatos költségtérítés összegének meghatározása során alkalmazandó önköltség számítási szabályok szerint követelheti az érintettől.

88. A költségtérítés megállapításánál a közérdekű adatok megismerésére irányuló igények teljesítésére vonatkozó költségtérítési szabályokat kell alkalmazni.

21. Eljárás a NAIH fellépése esetén

89. Amennyiben a BAZ VMKI-nál a NAIH

a) vizsgálatot,

b) adatvédelmi hatósági eljárást vagy

c) titokfelügyeleti hatósági eljárást

indít, az érintett adatkezelő szerv adatvédelmi tisztviselője a BM OKF adatvédelmi tisztviselőjét – a szolgálati út betartásával – haladéktalanul értesíti.

90. A NAIH vizsgálatával, valamint az adatvédelmi és a titokfelügyeleti hatósági eljárással érintett adatkezelő szervezeti egység vezetője köteles a NAIH részére

a) minden szükséges tájékoztatást szóban és írásban megadni,

b) az összes olyan iratba való betekintést és a 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.

91. Az adatkezelő a 91. pontban meghatározott kötelezettségeinek az Infotv. 54. § (2) bekezdésében meghatározott határidőig köteles eleget tenni.

92. Az adatkezelő, illetve a tájékoztatásra felkért személy a tájékoztatást az Infotv. 54. § (3) bekezdése alapján tagadhatja meg.

93. A hivatásos katasztrófavédelmi szerv a NAIH vizsgálata alapján a személyes adatok kezelésével, illetve közérdekű adatok vagy közérdekből nyilvános adatok megismeréséhez fűződő jogok gyakorlásával kapcsolatos jogsérelem vagy annak közvetlen veszélye fennállását megalapozottnak tartó megállapításával való egyetértése vagy egyet nem értése esetén az Infotv. 56. § (2) bekezdésében foglaltak szerint jár el.

94. Ha a hivatásos katasztrófavédelmi szerv vezetője a NAIH adatvédelmi és titokfelügyeleti hatósági eljárásban hozott határozatát nem fogadja el, adatvédelmi hatósági eljárás esetén az adatvédelmi tisztviselő, titokfelügyeleti hatósági eljárás esetén a biztonsági vezető véleményének kikérését követően a bírósági felülvizsgálat kezdeményezésére nyitva álló határidőn belül a bírósághoz fordulhat.

95. A keresetindítási határidő lejártáig, illetve közigazgatási per indítása esetén a bíróság jogerős határozatáig a vitatott adatkezeléssel érintett adatok nem törölhetők, illetve nem semmisíthetők meg, az adatok kezelését a NAIH határozatának kézhezvételekor, illetve a NAIH eljárásának megkezdésekor fel kell függeszteni és az adatokat zárolni kell.

IV. Fejezet

22. A hivatásos katasztrófavédelmi szerv személyi állományába jelentkezők személyes adatainak kezelése, az új belépők tájékoztatása

96. A BAZ VMKI által az álláshely meghirdetésekor az adatkezelési tájékoztatásra vonatkozó általános szabályok szerint tájékoztatni kell a lehetséges pályázókat az adatkezelés körülményeiről.

97. Annak érdekében, hogy a nem pályázati kiírás eredményeként érkező önéletrajz benyújtója személyes adatok védelméhez fűződő joga ne sérüljön, a hivatásos katasztrófavédelmi szervek honlapján az önéletrajzok kezelésével és tárolásával kapcsolatos tájékoztatót kell elhelyezni az Álláspályázatok link alatt. A BAZ VMKI kizárólag annak vizsgálatára jogosult, hogy a pályázati anyagnak megfelelő betöltetlen álláshellyel rendelkezik-e, amennyiben ilyen álláshely nem áll rendelkezésre, az anyagot a benyújtójának vissza kell küldeni vagy meg kell semmisíteni.

98. Az önéletrajzok tárolási ideje az adott pályázat lezárulásától, amennyiben a jelentkezés pályázattól függetlenül érkezett, a jelentkezés benyújtásától számított 3 hónap. Ennek elteltét követően az anyagban a személyes adatokat felismerhetetlenné kell tenni.

99. Az adattárolási határidő lejártát követően a pályázati anyagokat meg kell semmisíteni, ha arra a jelentkező külön igényt tart, részére vissza kell küldeni. Az adatmegsemmisítésről jegyzőkönyvet kell felvenni.

100. Az adatkezelő szerv adatvédelmi tisztviselője a szerv által végzett dolgozói adatkezelésekről tájékoztatót készít, amelyet az új állománytagok részére a munkába állást követően átad, vagy elektronikusan hozzáférhetővé tesz, amelynek tényéről és az elérési útról dokumentáltan tájékoztatja az állomány tagját. Az új állománytag az ismeretek átadását aláírásával igazolja.

23. Telefon- és internethasználat ellenőrzése

101. Az e-mail fiók ellenőrzésekor a tisztességes adatkezelés elvéből következően előzetesen tájékoztatni kell az állománytagot a tervezett munkáltatói intézkedésről, másrészt lehetőséget kell biztosítani számára, hogy ő vagy helyette meghatalmazottja vagy képviselője jelen legyen.

102. Az e-mail fiók áttekintésének körülményeit olyan módon kell jegyzőkönyvben rögzíteni, hogy annak pontos menete, az annak során megismert adatok köre, az elvégzett adatkezelési műveletek és azok jogszerűsége utólag ellenőrizhető legyen.

103. A munkahelyi internet- és telefonhasználat, valamint az elektronikus levelezés ellenőrzéséről egyebekben a hivatásos katasztrófavédelmi szervek Informatikai Biztonsági Szabályzata rendelkezik.

104. A vezetékes munkahelyi telefonok használatával kapcsolatos adatvédelmi kérdéseket a BM Országos Katasztrófavédelmi Főigazgatóság informatikai szakterületének Gazdálkodási Szabályzatáról szóló BM OKF főigazgatói intézkedés rendezi.

24. Nem állománytagokról készült kép- vagy kép- és hangfelvételekkel kapcsolatos adatkezelés

105. A BAZ VMKI állományába nem tartozó személyekről készítendő kép- vagy kép- és hangfelvételeken történő részvétel kapcsán a képmásnak mint személyes adatnak kezelésére – törvényi felhatalmazás hiányában – kizárólag az érintett előzetes hozzájárulásával kerülhet sor. Az érintettek hozzájárulását nem kell megszerezni, ha a felvétel

a) nyilvános közéleti szereplés során készült felvételnek vagy tömegfelvételnek minősül,

b) a hivatásos katasztrófavédelmi szerv által ellátott szolgálati feladattal összefüggésben hatósági ellenőrzés vagy beavatkozás során készül.

106. Amennyiben a felvétel készítőjének módjában áll megfelelő szóbeli tájékoztatást adni az adatkezelésről, az érintettek hozzájárulása szóban is beszerezhető.

107. A tájékoztatás és a hozzájárulás beszerzése során figyelemmel kell lenni a megfelelő adatkezelői szint(ek) megjelölésére és arra, hogy a hozzájárulás valamennyi nyilvánosságra hozatali helyre (a BM OKF, a területi szervek honlapja, a Médiaszerver, a katasztrófavédelem Facebook-oldala és Youtube-csatornája, Instagram- és Twitter-profilja, a, Katasztrófavédelem című elektronikus magazin, a Katasztrófavédelem Központi Zenekar honlapja, a Katasztrófavédelem Központi Múzeum honlapja, a Katasztrófavédelmi Kutatóintézet honlapja, az Országos Katasztrófavédelmi Sportegyesület honlapja) kiterjedjen.

108. Rendezvények, események szervezése esetén a rendezvény, esemény szervezője lehetőség szerint előzetesen köteles gondoskodni az érintettek megfelelő tájékoztatásáról és a hozzájárulások beszerzéséről.

25. Mozgó kamerák

109. A beavatkozás-elemzési, oktatási célból telepített kamera esetében, amennyiben a kamera a személyeket azonosítható módon rögzíti (pl. álló jármű elé kerülő személyek), és a felvételeket a hivatásos katasztrófavédelmi szerv később fel kívánja használni, de a felhasználási cél az arcképek kezelését nem indokolja, olyan technikai hátteret kell biztosítani, amely alkalmas a személyazonosításra alkalmas felvételek anonimizálására.

110. A beavatkozás-elemzési, oktatási célból telepített kamera által rögzített felvételt illetéktelen személyeknek átadni, valamint a felvételt nyilvánosságra hozni nem lehet, kivétel a felvétel oktatási célból történő bemutatása. A személyes adatokat azonban ilyenkor is felismerhetetlenné kell tenni.

111. A BAZ VMKI gépjárművébe a szolgálatteljesítést ellenőrző technikai eszközként telepített képfelvevő által rögzített felvétel megismerésére az állományilletékes parancsnok és az általa erre munkakörüknél fogva kijelölt személyek jogosultak, az még oktatási célra sem használható fel, törvényi felhatalmazás hiányában nem bocsátható harmadik személyek rendelkezésére. A képfelvevő felszereléséről az adott gépjárművön szolgálatot teljesítő állományt előzetes írásbeli tájékoztatásban kell részesíteni.

112. A felvételen látható gépjármű rendszámát kizárólag abban az esetben kell kitakarni, amennyiben az magánszemély gépjárműve. A BAZ VMKI és más közfeladatot ellátó szervek, személyek gépjárművei esetén a kitakarásra nincs szükség.

113. A kamerával rendelkező gépjármű kamerájának üzemeltetéséért felelős személy a gépjárművezető.

114. Ha a gépjármű mozgása során valamely különleges esemény történik, a kamera által rögzített eseményről készült felvételt a szolgálati elöljárónak át kell adni.

115. A gépjármű és a kamera használói, kezelői adatvédelmi oktatásban részesülnek az adatvédelmi tisztviselőtől a kamera üzemeltetési köre és a felvételek anonimizálása tekintetében.

116. Az adatvédelmi tisztviselő bármikor jogosult betekinteni a kamera felvételeibe ellenőrzés céljából.

117. A BAZ VMKI objektumain található mozgó kamerái kizárólag magánterületen, illetve a magánterületnek a közönség számára nyilvános részén használhatók.

26. Hatósági tevékenységgel kapcsolatos adatkezelési szabályok

118. A hatósági ügyekkel kapcsolatos személyesadat-kezelés az általános közigazgatási rendtartásról szóló 2016. évi CL. törvény (a továbbiakban: Ákr.) és az adott hatósági ügytípusra irányadó adatkezelési szabályok szerint történik.

119. Az ügyfél és az eljárás egyéb résztvevőjét tájékoztatni kell a zárt adatkezelés lehetőségéről és annak indokairól. Az ügyfél és az eljárás egyéb résztvevője természetes személyazonosító adatainak és lakcímének zárt kezelését úgy kell biztosítani, hogy a védett személy adatait tartalmazó eredeti iratokat az ügy iratai között elkülönítetten, zárt, lepecsételt borítékban kell elhelyezni.

120. A kiskorú, cselekvőképtelen vagy cselekvőképességében részlegesen korlátozott nagykorú ügyfél, tanú, szemletárgy-birtokos vagy megfigyelt személy érdekében a hatóság a kiskorú, a cselekvőképtelen és a cselekvőképességében részlegesen korlátozott nagykorú ügyfél, tanú, szemletárgy-birtokos vagy megfigyelt személy védelme érdekében erre irányuló kérelem nélkül is dönthet az érintett személy adatainak zárt kezeléséről és az irat betekintési jog korlátozásáról.

121. A zártan kezelt adatok megismerésére a hatóság, a felügyeleti szerv, valamint a fellebbezés elbírálására jogosult hatóság, az illetékes ügyész és a bíróság jogosult.

122. Ügyféli minőség hiánya esetén iratbetekintést kérő személy személyes adatot tartalmazó iratba kizárólag akkor tekinthet be, ha az adat megismerése joga érvényesítéséhez, kötelezettsége teljesítéséhez szükséges, ellenkező esetben a kérelmet el kell utasítani.

123. Ha törvény a döntés nyilvánosságát nem korlátozza vagy nem zárja ki, és az igénylő az eljárás befejezését követően a véglegessé vált határozatot, valamint az elsőfokú határozatot megsemmisítő és az elsőfokú határozatot hozó hatóságot új eljárásra utasító végzést szeretné megismerni, akkor csak a személyes adatot és a védett adatot nem tartalmazó iratot ismerheti meg.

124. A közérdekű bejelentés vagy panasz alapján indult hatósági eljárást lezáró, már véglegessé vált döntés megismerhetősége nem zárható el a korábbi bejelentőtől vagy panaszostól arra hivatkozással, hogy az anonimizált határozat kivonatából következtetések vonhatóak le az ügyfél személyére nézve, mivel a közérdekű bejelentést vagy panaszt benyújtó személy az ügyfelet nyilvánvalóan ismeri.

125. A törvény alapján kötelezően közzéteendő végleges vagy fellebbezésre tekintet nélkül végrehajthatóvá nyilvánított hatósági határozatok közzétételének adatvédelmi szabályait külön intézkedés határozza meg.

27. Beavatkozásokkal kapcsolatos adatkezelési szabályok

126. A tűz elleni védekezésről, a műszaki mentésről és a tűzoltóságról szóló 1996. évi XXXI. törvény 10/A. § (2) bekezdésében rögzített adatokat tartalmazó iratanyagot a hivatásos tűzoltóságokon és katasztrófavédelmi őrsökön elzárva kell tárolni.

V. Fejezet

Adatbiztonsági előírások

28. Adatbiztonsági intézkedések

127. Az adatbiztonsági intézkedéseket – a vonatkozó jogszabályok és a Szabályzat keretei között – valamennyi hivatásos katasztrófavédelmi szervnél a biztonságos adatkezeléshez és a helyi adottságokhoz igazodva kell meghatározni és végrehajtani.

128. Az infrastruktúrához, a hivatásos katasztrófavédelmi szerv objektumaihoz kapcsolódó és a hardvereszközök védelmét szolgáló adatbiztonsági követelményekről, valamint az informatikai rendszerekben tárolt adatok védelméről az Informatikai Biztonsági Szabályzat és külön belső szabályozók rendelkeznek.

129. A személyes adatok kezelésére vonatkozó szigorúbb előírásokat a személyes adatok kezelése figyelembevételével történt magasabb információbiztonsági kockázati osztályba sorolás kezeli.

29. Az adatkezelés dokumentációjának védelmére vonatkozó adatbiztonsági intézkedések

130. A személyes adatokat tartalmazó adatállományok dokumentációit nyilvántartásba kell venni és gondoskodni kell azok aktualizálásáról. Meg kell határozni a dokumentációkhoz történő hozzáférésre jogosultak körét, egyébként a hozzáférés csak az adatkezelő szerv vezetőjének engedélyével történhet. Szabályozni kell a dokumentációk tárolásának, másolásának, esetleges kölcsönzésének rendjét.

131. A személyes adatokat és a személyes adatok különleges kategóriáit tartalmazó adatkezelések dokumentációit páncélszekrényben vagy biztonsági zárral és falakattal ellátott lemezszekrényben, vagy biztonsági zárral, vasráccsal és falakattal, illetve elektronikus védelemmel ellátott helyiségben kell őrizni.

30. A személyhez fűződő és az alkalmazói tevékenységgel összefüggő intézkedések

132. Az adatkezelő szerv vezetőjének gondoskodnia kell a személyes adatok kezelését végző állomány megfelelő képzéséről és továbbképzéséről.

133. A számítógépes hálózaton személyes adatokat tartalmazó dokumentumot kizárólag abban az esetben lehet több személy által is hozzáférhető mappában elhelyezni, amennyiben a személyes adatot tartalmazó irat a mappához hozzáférési jogosultsággal bíró szervezeti egység állományának feladatkörébe tartozó ügytípus ügyirata.

VI. Fejezet

Információszabadság a hivatásos katasztrófavédelmi szerveknél

31. Az információszabadság tartalma

134. A BAZ VMKI-nak és személyi állományának lehetővé kell tennie, hogy az Infotv.-ben meghatározott kivételekkel a kezelésében lévő közérdekű adatot és közérdekből nyilvános adatot (a továbbiakban együtt: közérdekű adat) erre irányuló igény alapján bárki megismerhesse.

135. A közérdekű adatokhoz történő hozzáférés biztosítható közzététellel, különösen a közérdekű adatokat kezelő szerv honlapján és az Egységes Közadatkereső Rendszerben, vagy erre irányuló egyedi igény megválaszolásával.

136. Az adatkezelő szerv vezetőjének döntése alapján a közérdekű adatok írásban megjelölt körét az előírt módon külön erre irányuló kérelem hiányában is nyilvánosságra kell hozni. Az adatkezelő szerv vezetője általi döntés alapján nyilvánosságra hozandó adatok körére bármely szervezeti elem javaslatot tehet, különösen akkor, ha ugyanazon témában több helyről érkezik adatigény vagy sajtómegkeresés.

32. Szerződésekkel, támogatásokkal kapcsolatos adatnyilvánosság és az üzleti titok

137. A hivatásos katasztrófavédelmi szervekkel szerződéses kapcsolatban álló szervekkel, személyekkel kötött szerződésekben az alábbiakat kell feltüntetni: „A szerződő felek tudomásul veszik, hogy az Infotv. 27. § (3)–(3a) bekezdése alapján a szerződés tartalma közérdekű, illetve közérdekből nyilvános adatnak minősül, és az nem minősül üzleti titoknak. Az esetleges nyilvánosságra hozatal azonban nem eredményezheti az olyan adatokhoz – így különösen a védett ismerethez – való hozzáférést, amelyek megismerése az üzleti tevékenység végzése szempontjából aránytalan sérelmet okozna, feltéve hogy ez nem akadályozza meg a közérdekből nyilvános adat megismerésének lehetőségét. A felek az arra irányuló kérelem esetén kötelesek a szerződés közérdekű, illetve közérdekből nyilvános adatnak minősülő tartalmára vonatkozóan tájékoztatást adni."

138. A hivatásos katasztrófavédelmi szerv által kiadási előirányzat terhére kötött visszterhes szerződésekben az alábbiakat kell feltüntetni: „A szerződő felek tudomásul veszik, hogy a kötelezettséget vállaló az átláthatóság ellenőrzése céljából, a szerződésből eredő követelések elévüléséig az államháztartásról szóló 2011. évi CXCV. törvény 41. § (6) bekezdése és az 55. §-a alapján jogosult a jogi személy, jogi személyiséggel nem rendelkező szervezet átláthatóságával összefüggő, az 55. §-ban meghatározott adatok kezelésére, amelyből a b) pont ba)–bc) alpontjában és a c) pont ca) és a cd) alpontjában foglalt adatok személyes adatnak minősülnek, amelyek tekintetében az adatkezelés kötelező."

139. Az állami vagyonnal való gazdálkodásra és az azzal való rendelkezésre vonatkozó szerződések esetén a szerződésben az alábbiakat kell feltüntetni: „A szerződő felek tudomásul veszik, hogy az állami vagyonról szóló 2007. évi CVI. törvény 5. § (1) bekezdése alapján a

szerződés közérdekű adatnak nem minősülő tartalma közérdekből nyilvános adat, ha külön törvény másként nem rendelkezik."

33. A közérdekű adatok megismerésére irányuló igények, az Alapvető Jogok Biztosának Hivatalától, valamint az országgyűlési képviselőktől érkező megkeresések intézésének eljárási szabályai és a költségtérítés

140. Közérdekű adat megismerése iránt bárki szóban, írásban vagy elektronikus úton terjeszthet elő igényt.

141. A BAZ VMKI adatvédelmi tisztviselője intézi a területi és a helyi szerv által kezelt adatokra irányuló közérdekűadat-megismerési igényeket, amennyiben a kérelem nem valamennyi hivatásos katasztrófavédelmi szerv által kezelt vagy a BM OKF-fel közösen kezelt adat kiadására irányul. Amennyiben a kért adatok besorolása nem egyértelmű vagy az ügy bonyolultsága azt indokolja, a területi adatvédelmi tisztviselő a BM OKF információszabadsággal foglalkozó tisztviselőjének állásfoglalását kéri.

142. A területi adatvédelmi tisztviselő a kérelem beérkezéséről, ideértve az Alapvető Jogok Biztosának Hivatalától, valamint az országgyűlési képviselőktől érkező megkereséseket is, a BM OKF információszabadsággal foglalkozó tisztviselőjét haladéktalanul értesíti, a közérdekűadat-megismerési igény esetén azt szerkeszthető formátumban is megküldi. A BM OKF információszabadsággal foglalkozó tisztviselője koordinálja a hivatásos katasztrófavédelmi szerveknek a közérdekű adatok megismerésére irányuló kérelmek, az Alapvető Jogok Biztosának Hivatalától, valamint az országgyűlési képviselőktől érkező megkeresések teljesítésével kapcsolatos tevékenységét. A koordináció lezárultát követően a BM OKF információszabadsággal foglalkozó tisztviselője megküldi a jóváhagyott választ a területi adatvédelmi tisztviselő részére, aki gondoskodik annak megküldéséről az adatigénylő, az Alapvető Jogok Biztosának Hivatala vagy az országgyűlési képviselő részére.

143. A BM OKF információszabadsággal foglalkozó tisztviselője és a területi adatvédelmi tisztviselő 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.

144. 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 BM OKF információszabadsággal foglalkozó tisztviselője, illetve a területi adatvédelmi tisztviselő felhívja az igénylőt az igény pontosítására.

145. A BM OKF információszabadsággal foglalkozó tisztviselője és a BAZ VMKI adatvédelmi tisztviselője az igény pontosításának elmulasztása esetén figyelmezteti az adatigénylőt arra, hogy amennyiben a pontosítást elmulasztja, igényének teljesítése részben vagy egészben meghiúsul.

146. Az igényelt adatot tartalmazó nyilvános forrás megjelölése kizárólag abban az esetben helyettesíti az igény teljes egészében történő megválaszolását, amennyiben a nyilvánosságra hozott adatok megegyeznek a kiadni kért adatokkal.

147. Amennyiben az igényelt adat kezelője nem a megkeresett szerv, és az igényelt közérdekű adatot kezelő szerv a megkeresett szerv előtt ismert, erről a tényről, azon szerv megjelölésével, amelytől a kért adat igényelhető, az igénylőt tájékoztatni kell.

148. 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 BM OKF információszabadsággal foglalkozó tisztviselője és a területi adatvédelmi tisztviselő az igény kézhezvételétől számított 15 napon belül tájékoztatja a határidő meghosszabbításának okáról.

149. Ha az igénylő az adatokat tartalmazó dokumentumról vagy dokumentumrészről másolatot kíván kérni, valamint ha az adatigény teljesítése a közfeladatot ellátó szerv alaptevékenységének ellátásához szükséges munkaerőforrás aránytalan mértékű igénybevételével jár, az adatkezelő hivatásos katasztrófavédelmi szerv költséget állapíthat meg.

150. A költségtérítés megállapításánál az Infotv. 29. § (5) bekezdésében felsorolt költségelemek vehetők figyelembe, a közérdekű adat iránti igény teljesítéséért megállapítható költségtérítés mértékéről szóló 301/2016. (IX. 30.) Korm. rendeletben foglaltak szerint.

151. A dologi költségek számítási módját a hivatásos katasztrófavédelmi szervekhez érkezett közérdekűadat-megismerési igények teljesítésével kapcsolatos költségtérítés összegének meghatározása során alkalmazandó önköltség számítási szabályokról szóló Tolna VMKI igazgatói intézkedés tartalmazza.
153. A dologi költségekről a Költségvetési Osztály állít ki számviteli bizonylatot.

154. A dologi költségek megállapítására van lehetőség a közérdekű adatok megismerésére vonatkozó adatigény teljesítésekor.

155. A BAZ VMKI adatvédelmi tisztviselője az adatigény megválaszolásában érintett szervezeti elemnek megküldi a hivatásos katasztrófavédelmi szervekhez érkezett közérdekűadat-megismerési igények teljesítésével kapcsolatos költségtérítés összegének meghatározása során alkalmazandó önköltség számítási szabályokról szóló BAZ VMKI igazgatói intézkedésben meghatározott dokumentumot az adatigénnyel együtt.

156. Ha a dologi költségek vonatkozásában a másolandó oldalak száma a 10 oldalt meghaladja, e-mailben az igényelt közérdekű adatot kezelő szervezeti elem vezetője megküldi a hivatásos katasztrófavédelmi szervekhez érkezett közérdekűadat-megismerési igények teljesítésével kapcsolatos költségtérítés összegének meghatározása során alkalmazandó önköltség számítási szabályokról szóló BAZ VMKI igazgatói intézkedésben meghatározott dokumentumot a Költségvetési Osztály vezetőjének a költségszámítás elkészítése céljából.

157. A Költségvetési Osztály a rendelkezésre álló tényleges dologi költségek feltüntetése után, a hivatásos katasztrófavédelmi szervekhez érkezett közérdekűadat-megismerési igények teljesítésével kapcsolatos költségtérítés összegének meghatározása során alkalmazandó önköltség számítási szabályokról szóló BAZ VMKI igazgatói intézkedésben meghatározott

dokumentumot megküldi a BAZ VMKI adatvédelmi tisztviselő részére a költségek összegszerű kimutatásával.
158. A BAZ VMKI adatvédelmi tisztviselője a várható dologi kiadások összegéről a közérdekű adat megismerésére vonatkozó igény beérkezésétől számított 15 napon belül tájékoztatást küld az adatigénylő részére.
159. Ha az a dokumentum vagy dokumentumrész, amelyről az igénylő másolatot igényelt, jelentős terjedelmű, illetve a költségtérítés mértéke meghaladja a kormányrendeletben meghatározott összeget, az adatigénylést a költségtérítésnek az igénylő általi megfizetését követő 15 napon belül kell teljesíteni.

160. A tájékoztatásnak ki kell terjednie arra, hogy amennyiben az adatigénylő a tájékoztatásban foglaltakat elfogadja, a költség elfogadásától számított 15 napon belül köteles azt befizetni az adatkezelő hivatásos katasztrófavédelmi szerv által írásban meghatározott folyószámlaszámra.

161. A BAZ VMKI adatvédelmi tisztviselője a számviteli bizonylat elkészítése céljából az adatigénylőnek – a költségekről szóló tájékoztatóval egy időben – megküldi a 3. függelékben meghatározott dokumentumot, amelyen az adatigénylő nevét és címét szükséges feltüntetni a számviteli bizonylat kiállítása céljából.

162. Az igény teljesítése során kiemelt figyelmet kell fordítani arra, hogy a közérdekű adatok közlése ne járjon mások jogainak vagy törvény alapján korlátozottan megismerhető adatok bizalmasságának sérelmével. Különös figyelmet kell fordítani arra, hogy az adatszolgáltatással ne kerüljenek nyilvánosságra személyes adatok, minősített adatok, törvény által nyilvánosságában korlátozott vagy – ha az adatkezelő szerv vezetője másként nem döntött – döntés-előkészítő, nem nyilvános adatok.

163. Ha a közérdekű adatot tartalmazó dokumentum az igénylő által meg nem ismerhető adatot is tartalmaz, a másolaton a meg nem ismerhető adatot felismerhetetlenné kell tenni, olyan módon, hogy a korlátozottan megismerhető adatok tartalmára megalapozott következtetést ne lehessen levonni. A meg nem ismerhető adatok kitakarása során figyelemmel kell lenni arra is, hogy az igénylő által megismerhető adatok ne essenek kitakarás alá.

164. A közérdekű adatigényekről, az abban szereplő adatkörökről a területi adatvédelmi tisztviselő negyedévente egyeztet a BM OKF információszabadsággal foglalkozó tisztviselőjével. Az elutasított kérelmekről, valamint az elutasítások indokairól a BM OKF információszabadsággal foglalkozó tisztviselője, illetve a területi adatvédelmi tisztviselő nyilvántartást vezet, és az abban foglaltakról a tárgyévet követő év január 31-éig tájékoztatja a NAIH-ot.

165. A közérdekű vagy közérdekből nyilvános adat kiadására irányuló sajtó- és média megkeresések intézésébe a hivatásos katasztrófavédelmi szerv szóvivője a BAZ VMKI adatvédelmi tisztviselőjét bevonja.

166. Az igénylés alapján történő adatszolgáltatás esetén az adatigénylő személyazonosító adatai csak annyiban kezelhetőek, amennyiben az az igény teljesítéséhez – beleértve az esetleges költségek megfizetését és az azonos igénylőtől, egy éven belül beérkezett jelleg ellenőrzését – elengedhetetlenül szükséges.

167. Az adatigény beérkezésétől számított 1 éves időtartam lejártát követően az igénylő személyes adatait haladéktalanul törölni kell. A törlésről az ügy előadója kitakarással gondoskodik.

34. A hatósági ügyekkel kapcsolatban érkező adatigények megválaszolására vonatkozó szabályok

168. Ha az adatigény folyamatban lévő hatósági ügyet érint, a megválaszolásakor az Ákr. irat betekintési rendelkezéseiben foglalt korlátozásokat is figyelembe kell venni. Erre a válasziratban fel kell hívni az adatigénylő figyelmét.

169. Ha az igény olyan hatósági eljárás kapcsán érkezik, amely még folyamatban van, az Infotv. 27. § (5) bekezdése döntés előkészítő iratokra vonatkozó rendelkezése, továbbá az Ákr. 34. § (1) bekezdése alapján – miszerint nem lehet betekinteni a döntés tervezetébe – meg kell tagadni az igény teljesítését, és felhívni az igénylő figyelmét, hogy megkeresését későbbiekben az Ákr. 33. § (5) bekezdése értelmében nyújthatja be az adatkezelő hivatásos katasztrófavédelmi szervhez.

170. A hatósági ügyekre vonatkozó adatigények esetén az Ákr. 33. § (5) bekezdése alapján bárki számára megismerhető határozatok, azok véglegessé válásáról szóló feljegyzéssel (záradékkal), vagy a véglegessé válásról szóló külön tájékoztatással egyidejűleg adhatók ki az anonimizálási szabályok betartásával, egyébként bármely más irat tekintetében fel kell hívni az adatigénylőt az Ákr. szerinti iratbetekintési jog gyakorlására.

.

171. Amennyiben a megkeresés nem iratok, hanem információk kiadására irányul, figyelemmel kell lenni arra, hogy az adott információ mely iratból származik. Ha nem adható válasz a kérdésre a jogerős határozat tartalma alapján, fel kell hívni az adatigénylőt Ákr. szerinti irat betekintési jog gyakorlására.

172. Ha az adatigény azért nem teljesíthető, mert a hivatásos katasztrófavédelmi szerv az Ákr. szerinti irat betekintési jog gyakorlására hívja fel az adatigénylőt, a válasz az igény teljesítésének részben vagy egészben történő megtagadásának minősül, ennélfogva az igénylőt tájékoztatni kell a jogorvoslati lehetőségekről.

35. A közérdekű adatok elektronikus úton történő közzététele

173. Az elektronikus információszabadság megvalósítása érdekében a BAZ VMKI honlapján közzétételi listákat működtet.

174. A listák tartalmának honlapon történő elhelyezéséről a honlap szerkesztéséért felelős szóvivő gondoskodik.

175. A közzétételi listákat a nyitólapról közvetlenül elérhető oldalon, „Közérdekű adatok" hivatkozás alatt kell közzétenni. A honlapon az Egységes Közadatkereső Rendszerre, a Központi Elektronikus Jegyzékre mutató hivatkozást is el kell helyezni.

176. Az általános közzétételi listában az adott hivatásos katasztrófavédelmi szerv vonatkozásában értelmezhetetlen közzétételi egységeket is fel kell tüntetni, de a pontos tájékoztatás érdekében jelezni kell, hogy az adott közérdekű adat a szervnél nem áll rendelkezésre.

177. A frissített adatok új állapota mellett fel kell tüntetni a frissítés tényét és idejét, illetve az adat előző állapotának archív állományban való elérhetőségét.

178. Amennyiben a közzétételi lista az adat előző állapotának archívumban tartását írja elő, az adat frissítése esetén annak elérhetővé tétele a megőrzési idő elteltéig nem szüntethető meg, és az adat mellett fel kell tüntetni a frissítés tényét és idejét, az új állapot fellelhetőségét, valamint feltűnő módon azt, hogy az archívumban elérhető adat nem időszerű.

179. A kötelező archiválási idő elteltét követően az adatfelelős szerv döntést hoz az adat törléséről vagy archívumban tartásáról.

180. A közzétételi lista által előírt megőrzési kötelezettség lejártakor a BM OKF információszabadsággal foglalkozó tisztviselője, illetve a területi adatvédelmi tisztviselő a közzétett, külön jogszabályban meghatározott közzétételi egységeket átadja a központi elektronikus jegyzék működtetője részére.

181. A BAZ VMKI a 4. függelék alapján készíti el közzétételi listáit.

182. A közzétételi listában nem szereplő közérdekű adatokra vonatkozó adatigénylések adatai alapján a BAZ VMKI adatvédelmi tisztviselője legalább évente felülvizsgálja a hivatásos katasztrófavédelmi szerv egyedi közzétételi listáját, és a jelentős arányban vagy mennyiségben felmerült adatigénylések alapján azt kiegészíti.

183. Az adatfelelős szervezeti elemeket és személyeket a területi szervek saját hatáskörben határozzák meg.

184. A BAZ VMKI-nál az adatfelelős személyek a közzétételi listákban meghatározott adatokat közvetlenül vagy az adatfelelős szervezeti elem útján, elektronikus úton küldik meg a BAZ VMKI adatvédelmi tisztviselőjének és a szóvivőnek, aki gondoskodik a továbbított közérdekű adatok honlapon történő nyilvánosságra hozataláról.

185. Az adatfelelős személyek gondoskodnak a közreműködésükkel közzétett adatok naprakészségének figyelemmel kíséréséről, és szükséges esetben a közzétételi listán adott adatfajtára meghatározott időközönként – azonnali adatfrissítést előíró rendelkezés esetén a változást követő munkanapon – történő frissítésének, a korábbi adatok archiválásának, továbbá, amennyiben a kötelező archiválási idő már eltelt, és az információ honlapon történő megjelenítése már nem indokolt, az archívumból történő törlés kezdeményezéséről.

186. A közzétételi listákba feltöltött adatok helytállóságáért és naprakészségéért az adatfelelős személy, a kapott adatok feltöltéséért az adatközlő, a listák egyes részei feltöltöttségének ellenőrzéséért a BAZ VMKI adatvédelmi tisztviselője felel.

187. A helyi szervek – mint adatfelelősök – a tevékenységükre vonatkozó közérdekű adatokat a felettes területi szervnek küldik meg. A területi szerv az alárendeltségébe tartozó helyi szervek vonatkozásában gondoskodik a megküldött közérdekű adatok közzétételéről.

188. Az adatfelelős, valamint a holnapon adatközlést intéző személyek feladatait munkaköri leírásukban rögzíteni kell.

189. Az Egységes Közadatkereső Rendszerben és a Központi Jegyzékben történő közzétételt a BAZ VMKI szóvivője folyamatosan végzi. A területi adatvédelmi tisztviselő a Központi Információs Közadat-nyilvántartás elektronikus felületén az 4. függelék III. Gazdálkodási

adatok Támogatások, Szerződések és Egyéb kifizetések pontjaira vonatkozó adatszolgáltatást az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény szerinti személyre szabott ügyintézési felületen található elektronikus űrlap kitöltésével, valamint az Infotv. 37/C. § (2) bekezdése szerinti rögzítésre szolgáló kitöltött adatlap egyidejű csatolásával, továbbá azok Nemzeti Adatvagyon Ügynökség hivatali tárhelyére történő beküldésével teljesíti.

VII. Fejezet

36. Ellenőrzés

190. Az adatkezelési rendelkezések betartásának ellenőrzésére jogosult:

a) az adatkezelő szerv vezetője vagy az általa írásban kijelölt személy;

b) az adatkezelő szerv vagy a felettes szerv adatvédelmi tisztviselője;

c) a központi szakirányítást ellátó szerv vezetője által ellenőrzésre írásban kijelölt személy;

d) a BM OKF Ellenőrzési Szolgálatának és az adatkezelő szerv ellenőrzési szolgálata állományának erre írásban felhatalmazott tagja;

e) a belügyminiszter által írásban felhatalmazott személy;

f) a jogszabályban erre felhatalmazott személy.

191. Az ellenőrzésre feljogosított az ellenőrzés céljára figyelemmel az ellenőrzés érdekében minden olyan helyiségbe beléphet, ahol adatkezelés folyik, az adatkezelést végzőktől minden olyan kérdésben felvilágosítást kérhet, minden olyan adatkezelést megismerhet vagy abba betekinthet, amely az ellenőrzött szerv adatkezelési tevékenységével összefügg.

192. Az egyes szervek, szakterületek szakmai tevékenységét érintő átfogó ellenőrzéseknek ki kell terjedniük a szakmai feladatellátáshoz szükséges adatkezelések törvényességének ellenőrzésére is.

193. Az adatkezelő szerv adatvédelmi tevékenységének célellenőrzését a BM OKF adatvédelmi tisztviselője vagy az adatkezelő szerv szakirányítására jogosult szerv vezetője rendelheti el.

194. A naplózási kötelezettség teljesítésére automatikusan, elektronikusan kerül sor, amelyet az informatikai szakterület ellenőriz.

195. A BAZ VMKI adatvédelmi tisztviselője által végzett ellenőrzés elsősorban az alábbiakra terjed ki:

a) közzétételi listák állapota;

b) személyes adatok kezelése az ellenőrzött szerv szervezeti elemeinél;

c) adatkezelési tevékenységek nyilvántartásának állapota;

d) az ellenőrzött szerv, szervezeti elem által vezetett nyilvántartások adatvédelmi megfelelősége;

e) a Humán Szabályzatban foglalt adatvédelmi rendelkezések megtartása;

f) az adatbiztonság követelményeinek való megfelelés.

196. A BAZ VMKI adatvédelmi tisztviselője legalább negyedévente köteles ellenőrizni a szerv közzétételi listáinak feltöltöttségét.

197. A BAZ VMKI adatvédelmi tisztviselője ellenőrzi az adatkezelő szervnél kiosztott hozzáférési jogosultságok aktualizáltságát. Az ellenőrzést az adatvédelmi tisztviselő a szerv rendszergazdájával közösen köteles végrehajtani, annak lefolytatása során a jelszavak meghatározott időszakonkénti megváltoztatására vonatkozó kötelezettség teljesítését is ellenőrizni kell.

198. A BAZ VMKI adatvédelmi tisztviselője ellenőrzi a szakterületek adatkezelési tevékenységét és a dolgozói adatkezeléseket.

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

VIII. Fejezet

37. Oktatás, vizsgáztatás, tájékoztatás

200. A BAZ VMKI állományába újonnan került olyan személyeket, akik munkakörüknél fogva személyes adatokat kezelnek, az adatvédelmi tisztviselő – az adatkezelő szerv személyzeti feladatot ellátó szervezeti elemével történő rendszeres egyeztetés alapján – köteles az állományba vételt követő három hónapon belül adatvédelmi oktatásban részesíteni és részére a szükséges jogszabályokat, belső normákat és egyéb segédanyagokat rendelkezésre bocsátani.

201. Az adatvédelmi tisztviselő az adatkezelő szerv személyes adatok kezelését végző személyi állományát a bekövetkezett adatvédelmi tárgyú jogszabály- és normaváltozásokról köteles tájékoztatni, indokolt esetben – különösen a jelentősebb adatvédelmi tárgyú normaváltozások vagy az ellenőrzés során feltárt visszatérő vagy egyébként súlyos hiányosságok esetén – az érintett állomány kötelező adatvédelmi oktatását elvégezni.

202. Az adatvédelmi tisztviselő az adatkezelő szerv információszabadsággal összefüggő feladatok ellátásáért felelős személyi állományát a közérdekű adatok nyilvánosságával összefüggő jogszabály- és normaváltozásokról köteles tájékoztatni, indokolt esetben – különösen a jelentősebb normaváltozások vagy az ellenőrzés során feltárt visszatérő vagy egyébként súlyos hiányosságok esetén – az érintett állomány kötelező, információszabadság tárgyú oktatását elvégezni.

1. függelék

Kérdőív az előzetes kockázatelemzéshez

Első rész: Szükséges-e a hatásvizsgálat lefolytatása? Előzetes adatvédelmi kockázatelemzés

1. Használ vagy fejleszt-e olyan informatikai rendszert, amely személyes adatokat kezel?

Igen □ Nem □

2. Szükséges-e személyes adatokat gyűjteni a szolgáltatás működtetéséhez?

Igen □ Nem □

3. Megvalósul-e a korábbiaktól eltérő célú adatkezelés már meglévő személyes adatokkal kapcsolatban?

Igen □ Nem □

a) Alkalmaz új adatköröket gyűjtő technológiát, amely jelentős mértékben megváltoztatja az adatkezelést?

Igen □ Nem □

b) Ha releváns szervezeti változás következik be:

- az egyesülés, beolvadás vagy egyéb szervezeti átalakulás hatással van-e az adatbázisokra?

Igen □ Nem □

- ez a változás eredményezi új adatok kezelését vagy új nyilvánosságra hozatali eljárásokat?

Igen □ Nem □

c) Ha ez az információ már korábban be lett gyűjtve:

- érint-e új vagy nagy létszámú érintett csoportot?

Igen □ Nem □

- rögzít-e ezen felül további személyes adatot?

Igen □ Nem □

4. A szolgáltatás korlátozza-e az érintettek személyes adataikhoz való hozzáféréséhez fűződő jogait?

Igen □ Nem □

5. Tervezi-e egymást követő 12 hónapból álló időszak során nagyszámú érintettekre vonatkozó személyes adatainak kezelését?

Igen □ Nem □

6. Megvalósul-e különleges adatok, tartózkodási helyre utaló adatok, illetve gyermekekre vagy munkavállalókra vonatkozó, széleskörű nyilvántartási rendszerekben tárolt adatok kezelése?

Igen □ Nem □

7. Megvalósul-e profilalkotás, amelyre az érintett személy tekintetében joghatással bíró vagy az egyént hasonlóan jelentős mértékben érintő intézkedések épülnek?

Igen □ Nem □

8. Megvalósul-e egészségügyi ellátás nyújtására, járványügyi kutatásokra, mentális vagy fertőző betegségekre irányuló felmérésekre vonatkozó személyes adatok kezelése, amennyiben az adatok feldolgozására meghatározott egyénekre széles körben vonatkozó intézkedések vagy döntések meghozatala érdekében kerül sor?

Igen □ Nem □

9. Megvalósul-e nyilvánosság számára hozzáférhető területek (közterületek) nagyarányú, automatizált nyomon követése?

Igen □ Nem □

10. Megvalósul-e olyan adatkezelés, amely során a személyes adatok megsértése várhatóan hátrányosan érintené az érintett személyes adatainak, magánéletének, jogainak vagy jogos érdekeinek védelmét?

Igen □ Nem □

11. Az adatkezelő vagy adatfeldolgozó fő tevékenységei olyan eljárásokat foglalnak-e magukban, amelyek jellegüknél, alkalmazási területüknél, illetve céljaiknál fogva az érintettek rendszeres és rendszerszerű megfigyelését igénylik?

Igen □ Nem □

12. A személyes adatokat olyan jelentős számú személy számára teszi-e hozzáférhetővé, amely ésszerűen elvárható módon nem korlátozható?

Igen □ Nem □

13. Létrejön-e új azonosító vagy hozzáférési jogosultságot ellenőrző rendszer, például biometrikus azonosítás?

Igen □ Nem □

14. Megfigyelés alatt állnak-e az érintettek helyváltoztatás, másokkal való kommunikáció vagy egyéb magatartás tanúsítása közben?

Igen □ Nem □

15. Megvalósul-e automatizált adatfeldolgozás?

Igen □ Nem □

16. Személyes adatok védelmének növelése érdekében előír-e (ha volt ilyen) a korábbinál magasabb szintű adatbiztonsági követelményeket?

Igen □ Nem □

17. Személyes adatokkal való visszaélés megelőzése érdekében bevezetésre kerülnek-e új vagy módosított előírások?

Igen □ Nem □

18. Személyes adatok tárolásával kapcsolatban bevezetésre kerülnek-e új vagy módosított előírások?

Igen □ Nem □

19. Megvalósul-e tudományos kutatási vagy statisztikai célból történő adatkezelés?

Igen □ Nem □

20. Az adatkezelés kiterjed-e különleges adatokra?

Igen □ Nem □

21. Megvalósul-e bármilyen más, magánszférát érintő magatartás?

Igen □ Nem □

22. Végeztek-e már korábban hatásvizsgálatot? Ha a válasz igen, csatolja a dokumentumot!

Igen □ Nem □

Második rész: Előzetes hatásvizsgálat

1. Ki a tájékoztatásra kötelezett személy (név, telefonszám, e-mail-cím)? (Ha van adatvédelmi tisztviselő, akkor az ő adatai.)

2. Mutassa be a szolgáltatás működését, felépítését!

3. Ki az adatkezelő (név, telefonszám, e-mail-cím, postai cím)?

4. Mi az adatkezelés pontos címe/helye/webhelye? (Csak akkor töltse ki, ha az eltér az adatkezelő címétől!)

5. Mi az adatkezelés célja, módja és jogalapja?

6. Mi az adatkezelés időtartama?

7. Kíván-e adatfeldolgozót igénybe venni? Ha igen, mutassa be részletesen az adatfeldolgozó személyét (kapcsolattartó, adatkezeléssel összefüggő tevékenység, adatfeldolgozó címe, adatfeldolgozás helye, technológiája stb.)!

8. Melyek a kezelni kívánt adatkörök?

9. Határozza meg a gyűjteni kívánt adatok mennyiségét, illetve az érintett személyek számát (hozzávetőlegesen)!

10. Melyek az adatfelvétel formái? Megvalósulhat az adatgyűjtés személy azonosítására alkalmas igazolvány segítségével is? Ha igen, fejtse ki!

11. Az adatszolgáltatás önkéntes? Ha igen, az érintettek megfelelő mértékben tájékoztatva vannak-e a kezelt adatok köréről, illetve jogaikról?

12. Az érintetteknek van-e lehetőségük arra, hogy adataik kizárólag meghatározott célokra történő felhasználásához nyújtsanak hozzájárulást? Ha igen, hogyan?

13. Megvalósul-e harmadik országba irányuló adattovábbítás? Ha igen, írja le a továbbítandó adatok fajtáit, a továbbítás címzettjének adatait, valamint az adattovábbítás jogalapját!

14. Fejtse ki, milyen lépéseket tesz az adatok biztonságának megőrzése érdekében!

15. Ha megfelelő szintűnek vélt az adatok biztonsága, milyen eszközök óvják az azonosítatlan hozzáféréstől?

16. A megfelelő védelmi eszközöket használja azonosítatlan hozzáférés megakadályozása érdekében? Fejtse ki álláspontját!

17. Van egyéb közlendő információja?

Harmadik rész: További analízis

1. Hogyan biztosítja az érintettek jogainak érvényesítését?

2. Fejtse ki azokat az Ön által is ismert, alternatív megoldásokat, amelyek az eredeti eljáráshoz képest a cél elérése mellett kisebb mértékben érintenék a magánszférát!

3. Milyen módszerekkel kívánja csökkenteni az azonosított kockázati tényezőket?

4. Hogyan ellenőrzi az adatok teljességét?

5. Megfelelően naprakészek-e a gyűjtött adatok? Ha igen, támassza alá válaszát!

6. Kifejtett és részletezett az adatok természete?

7. Kinek van hozzáférési joga (lehetősége) a személyes adatokhoz?

8. Mi alapján kerülnek kiválasztásra azok a személyek, akik rendelkeznek ezzel a joggal?

9. A személyes adatokhoz való hozzáférés feltételei, módja, korlátai rögzítve vannak?

10. Milyen eszközök biztosítják az adatkezelés céljától eltérő felhasználás megakadályozását?

11. Hozzáférhet-e más rendszer a saját rendszerben kezelt adatokhoz? Ha igen, fejtse ki!

12. Az adatkezelés idejének lejárta után milyen módon kerülnek törlésre az adatok? Hogyan lesz dokumentálva az adattörlés?

2. függelék

Az adatvédelmi hatásvizsgálatról szóló összefoglaló jelentés tartalmi elemei

1. A tervezett vagy megváltozott adatkezelés leírása:

A tervezett/megváltozott adatkezelés folyamatának leírása, melyben bemutatásra kerülnek az alábbiak:

a) adatkezelés jellege, hatóköre, körülményei;
b) a személyes adatok, a címzettek, valamint a személyes adatok tárolási időtartamának meghatározása;
c) funkcionális leírás az adatkezelési műveletről;
d) módszeres leírás az adatfeldolgozásról, az adatkezelés céljainak ismertetésére, beleértve adott esetben az adatkezelő által érvényesíteni kívánt jogos érdeket;
e) jogalap meghatározása;
f) a személyes adatokhoz használt eszközök (hardverek, szoftverek, hálózatok, személyek, papírok vagy papíralapú továbbítási csatornák) megnevezése;
g) a kockázatok kezelését célzó intézkedések bemutatására, ideértve a személyes adatok védelmét és az e rendelettel való összhang igazolását szolgáló, az érintettek és más személyek jogait és jogos érdekeit figyelembe vevő garanciákat, biztonsági intézkedéseket és mechanizmusokat;
h) az adatkezelésre vonatkozó, rendelkezésre álló igazgatási rendszerterv, vagy folyamatleírás bemutatása;
i) hatásvizsgálatra vonatkozó szerep- és felelősségi körök meghatározása.

2. Az adatkezelési műveletek szükségességi és arányossági vizsgálata:

a) meghatározottak, kifejezettek és jogosak-e a cél(ok) [célhoz kötöttség elve – GDPR rendelet 5. cikk (1) bekezdés b) pontja];
b) az adatkezelés jogszerűsége (GDPR rendelet 6. cikke);
c) a kezelni kívánt adatok megfelelőek, relevánsak, és csak a szükséges adatokra korlátozódnak [adattakarékosság elve – GDPR rendelet 5. cikk (1) bekezdés c) pontja];
d) korlátozott tárolási időtartam [korlátozott tárolhatóság elve – GDPR rendelet 5. cikk (1) bekezdés e) pontja].

3. Meglévő vagy tervezett intézkedések: az adatkezeléssel összefüggő, a hatásvizsgálat elvégzésekor meglévő intézkedések felsorolása pl. jogosultság kezelés.

4. A jogokat és szabadságokat érintő kockázatok vizsgálata:

A kérdőívek kitöltése, valamint az érintettekkel történő esetleges konzultáció után a hatásvizsgálatot lefolytató szerv az adatkezelés minden releváns részelemének ismeretében elvégzi a kockázatkezelést, amelynek elemei az alábbiak:

a) a lehetséges kockázati tényezők azonosítása,
b) a kockázati tényezők értékelése,
c) a kockázati tényezők csökkentésére, megszüntetésére irányuló javaslatok megfogalmazása.

A kockázati tényezők azonosításában nagy szerepe van továbbá az érintettekkel való konzultációnak. A GDPR rendelet az érintettekkel való konzultációt nem szükségszerűen írja elő. Az adatkezelő „adott esetben" kéri ki az érintettek illetve képviselőik véleményét. Ha az adatkezelő végleges döntése eltér az érintettek véleményétől, akkor dokumentumokkal alá kell támasztania annak végrehajtásának vagy elvetésének okait. Az adatkezelőnek dokumentumokkal kell indokolnia azt is, hogy miért nem kéri ki az érintettek véleményét, amennyiben úgy dönt, hogy erre nincs szükség.

4.1. Konzultáció az érintett szereplőkkel

Azonosítani kell az érintett szereplők lehetséges körét, majd megfelelő mértékben tájékoztatni kell őket az eljárásról. A tájékoztatás célja – a visszajelzések útján – a negatív hatások csökkentése, illetve a figyelem felhívása a jogorvoslati lehetőségre. A tájékoztatás során ki kell térni az eljárás menetére, idejére, várt eredményére. Az esetleges konzultációt már a tervezési/fejlesztési szakaszban célszerű elvégezni, hogy az érintettek észrevételeit, ajánlásait esetlegesen implementálni lehessen, jelentős többletköltség nélkül. Az érintetti kör nincs korlátozva, a projekt tárgyát tekintve érintett lehet állami és civil szervezet, támogató, szolgáltató, fejlesztő és az adatkezelés adatalanyai egyaránt.

Az érintettek hatásvizsgálatba való bevonásának lehetőségei:

- az egyes érintett kategóriák meghatározása és párbeszéd folytatása az egyes kategóriák képviselőivel;

- konzultációs eljárások biztosítása, hogy az érintetteknek lehetőségük legyen álláspontjaik kifejtésére;

- a tervezet érintettek számára történő hozzáférhetővé tétele.

A konzultáció formája többféle lehet: interjú, közvélemény-kutatás, meghallgatás, workshop, online konzultáció.

A tervezett adatkezelés negatív hatásainak csökkentése vagy kiküszöbölése érdekében célszerű a visszajelzéseket dokumentálni és az adatkezelés megvalósítása során figyelembe venni.

4.2. A lehetséges kockázatok csoportjai

Személyeket érintő kockázatok:

- az adatok nem megfelelő nyilvánosságra hozatala növeli annak esélyét, hogy olyan adatokat is megosztanak, amelyeket jogszerűen nem lehetne;

- az adatkezelés célja megváltozhat, így az idő múlásával a tárolt adatokat másra használják fel az érintett tudta nélkül;

- adatbázisok összefésülése, amelynek köszönhetően olyan felhasználói profilok hozhatók létre, amelyekből új információk nyerhetők ki;

- azonosítók összekapcsolása, amely meggátolja az anonim felhasználást.

Szervezeteket érintő kockázatok:

- adatvédelmi hatóság álláspontjába vagy olyan jogszabályi előírásba való ütközés, amelynek következményeként bírság vagy más szankciók is kiszabhatók;

- olyan problémák felmerülése, amelyekre csupán a projekt elindítását követően derül fény, és a kijavításuk rendkívül költségigényes;

- az adatminimalizálás elvébe ütköző felesleges, készletező, esetleg többszöri adatgyűjtés, amely így csökkentheti a projekt hatékonyságát;

- a bizonytalan és nem megfelelő adatkezelés a társadalomban bizalomvesztést eredményezhet, amely bevételcsökkenés formájában jelenhet meg;

- adatvesztés, amely az érintettek számára kárt okoz, valamint az érintettek részéről kártérítési igényt generál.

Jogi szabályozásnak való megfelelés vizsgálata:

- az adatkezelés nem felel meg a tagállami hatóság állásfoglalásaiban foglaltaknak, az ágazat-specifikus előírásoknak vagy az alkotmányjogi előírásoknak.

4.3. Az adatvédelmi kockázatok rangsorolása

Az elemzés az 1. függelékben szereplő kérdéssor alapján azonosított kockázatok, és az érintett konzultáció értékelésével folytatódik. A magánszférára gyakorolt hatásuk mértéke alapján megkülönböztethető:

- alacsony (esély van a kockázat megjelenésére, de vannak enyhítő körülmények);

- közepes (valószínű, hogy megjelenik a kockázat, ha nem történik korrekció);

- magas (megjelenik a kockázat, ha nem történik korrekció) szintű kockázat.

Egy kockázat mértékét négy tényező befolyásolja:

A személyes adatkezelés alapját képező elektronikus információs rendszer kritikussága: nem kritikus=1 kritikus=2.

Az adatkezelés hatóköréhez tartozó adatokhoz képest (pl. az adott népesség aránya) az adatkezelés

1. kis számú =1,

2. közepes =2,

3. nagy számú =3

érintett adatkezelését valósítja meg.

A kockázat elhárításának ügyviteli sürgőssége: a bejelentő nem ítéli sürgősnek=1, a bejelentő sürgősnek ítéli=2.

Az adatkezelés fontossága (súlya) a szervezet szempontjából: kritikus=3, nem kritikus=1.

A kockázati szint számértékét a tényezők összege adja.

Ha az adott eseménynél egy tényező nem értékelhető, akkor a legkisebb számértéket kell használni.

A tényezők alapján három kockázati szint használható:

Magas = 8 vagy több

Közepes = 5–7

Alacsony = 4

4.4. A „valószínűsíthetően magas kockázattal járó" adatkezelési műveletek megállapítása

Értékelési szempontok:

- Értékelés vagy pontozás: ideértve a profilalkotást és az előrejelzést is, különösen „az érintett munkahelyi teljesítményére, gazdasági helyzetére, egészségi állapotára, személyes preferenciáira vagy érdeklődési körökre, megbízhatóságra vagy viselkedésre, tartózkodási helyére vagy mozgására vonatkozó jellemzők" alapján [GDPR rendelet (71) és (91) preambulum bekezdés]. Erre példaként említhető a pénzügyi vállalkozás, amely hitelreferencia-, pénzmosás és a terrorizmus finanszírozása elleni vagy csalásellenes adatbázist használ ügyfelei szűrésére, vagy a biotechnológiai vállalat, amely közvetlenül a fogyasztóknak kínál genetikai vizsgálatokat, hogy értékelje, és előre jelezze a betegségek kockázatát és az egészségügyi kockázatokat, vagy a vállalkozás, amely viselkedési vagy üzletszerzési profilokat készít a honlapjának használata vagy böngészése alapján.

- Joghatással vagy hasonló jelentős hatással járó automatizált döntéshozatal: adatkezelés, amelynek célja a „természetes személy tekintetében joghatással bíró" vagy „a természetes személyt hasonlóképpen jelentős mértékben érintő" döntések meghozatala [GDPR rendelet 35. cikk (3) bekezdés a) pontja]. Az adatkezelés adott esetben például egyének kirekesztését vagy hátrányos megkülönböztetését eredményezheti. Az egyénekre nézve csekély vagy semmilyen hatással nem járó adatkezelés nem felel meg ennek a konkrét szempontnak. Az itt említett fogalmakról további felvilágosítást nyújt majd a 29. cikk szerinti adatvédelmi munkacsoport soron következő, profilalkotásról szóló iránymutatása.

- Módszeres megfigyelés: érintettek megfigyelése, nyomon követése vagy ellenőrzése céljából végzett adatkezelés, többek között a hálózatokon keresztüli adatgyűjtés vagy a „nyilvános helyek nagymértékű, módszeres megfigyelése" [GDPR rendelet 35. cikk (3) bekezdés c) pontja]. Az ilyen jellegű megfigyelés azért tartozik a figyelembe veendő szempontok közé, mivel a személyes adatok gyűjtése olyan körülmények között folyhat, ahol előfordulhat, hogy az érintettek nem tudják, ki gyűjti és hogyan használja fel adataikat. Ezen kívül az egyéneknek talán nincs lehetőségük elkerülni, hogy közterületeken (vagy nyilvános helyeken) érintetté váljanak ilyen adatkezelésben.

- Különleges adatok vagy fokozottan személyes jellegű adatok: ide tartoznak a személyes adatok a GDPR rendelet 9. cikkében meghatározott különleges kategóriái (például az egyének politikai véleményére vonatkozó adatok), valamint a GDPR rendelet 10. cikkében meghatározott, büntetőjogi felelősség megállapítására vonatkozó határozatokra és a bűncselekményekre vonatkozó személyes adatok. Példaként említhető az általános kórház, amely nyilvántartást vezet a betegek kórtörténetéről, vagy a magánnyomozó, aki megőrzi az elkövetők adatait. Az GDPR rendelet e rendelkezésein túlmenően bizonyos adatkategóriák tekinthetők úgy, hogy fokozzák az egyének jogait és szabadságait érintő lehetséges kockázatokat. Ezek a személyes adatok (a fogalom általánosan ismert jelentését tekintve) különlegesnek minősülhetnek, mivel otthoni vagy magánjellegű tevékenységekhez

kapcsolódnak (például elektronikus hírközlési tevékenységekhez, amelyek bizalmassága védendő), kihatnak valamely alapvető jog gyakorlására (például helymeghatározó adatok, amelyek gyűjtése megkérdőjelezi a mozgás szabadságát), vagy az őket érintő jogsértések egyértelműen súlyos hatást gyakorolnak az érintett mindennapi életére (például pénzügyi adatok, amelyek csalásra használhatók). E tekintetben lényeges lehet, hogy az érintett vagy valamely harmadik személy már nyilvánosan hozzáférhetővé tette-e az adatokat. A személyes adatok nyilvános hozzáférhetősége az értékelés során egyik tényezőként figyelembe vehető, ha az adatok bizonyos célú további felhasználására lehet számítani. Ez a szempont olyan adatokra is vonatkozhat, mint például a személyes iratok, e-mailek, naplók, jegyzetelési funkcióval rendelkező e-olvasókból származó jegyzetek, valamint az életnaplózó alkalmazásokban tárolt, rendkívül személyes jellegű adatok.

- Nagy számban kezelt adatok: a GDPR rendelet nem határozza meg, mi értendő nagy szám alatt, jóllehet a GDPR rendelet (91) preambulum bekezdése nyújt némi iránymutatást. Mindenesetre a GDPR rendelet 29. cikke szerinti adatvédelmi munkacsoport ajánlása szerint különösen az alábbi tényezőket kell figyelembe venni annak megállapításakor, hogy az adatkezelés nagy számban történik-e:

a) az érintettek száma konkrét számadatként vagy a lakosság arányában;

b) a kezelt adatok mennyisége vagy adatfajták köre;

c) az adatkezelési tevékenység időtartama vagy állandó jellege;

d) az adatkezelési tevékenység földrajzi kiterjedése.

Adatkészletek egymással való megfeleltetése vagy összevonása például két vagy több, különböző célokból, illetve eltérő adatkezelők által végzett adatkezelési műveletből származó adatokkal, az érintett észszerű elvárásait meghaladó módon.

- Adatkészletek egymással való megfeleltetése vagy összevonása

- Kiszolgáltatott helyzetben lévő érintettekkel kapcsolatos adatok (GDPR rendelet (75) preambulum bekezdése): az ilyen jellegű adatok kezelése azért tartozik a figyelembe veendő szempontok közé, mivel nincs hatalmi egyensúly az érintettek és az adatkezelő között, ami azt jelenti, hogy az egyének adott esetben nem tudják adataik kezelését könnyen engedélyezni vagy ellenezni, illetve nem tudják a jogaikat gyakorolni. A kiszolgáltatott helyzetben lévő érintettek közé sorolhatók a gyermekek (ők úgy tekintendők, mint akik nem tudják tudatosan és átgondoltan ellenezni vagy engedélyezni adataik kezelését), a munkavállalók, a lakosság különleges védelmet igénylő, kiszolgáltatottabb helyzetben lévő rétegei (mentális betegségben szenvedők, menedékkérők vagy az idősek, betegek stb.), valamint az egyének minden olyan esetben, amikor az érintett és az adatkezelő közötti kapcsolatban egyenlőtlen helyzet alakul ki.

- Új technológiai vagy szervezési megoldások innovatív használata vagy alkalmazása: például az ujjlenyomat- és az arcfelismerés együttes használata a hatékonyabb beléptetés érdekében stb. Az GDPR rendelet egyértelműen megfogalmazza [, hogy „a technológia elismert állásának megfelelő" módon meghatározott új technológia használata szükségessé teheti az adatvédelmi hatásvizsgálat elvégzését [GDPR rendelet 35. cikk (1) bekezdése, (89) és (91) preambulum bekezdése]. Ennek oka, hogy az ilyen technológiák használatához újfajta adatgyűjtési és -felhasználási formák kapcsolódhatnak, ami magas kockázattal járhat az

egyének jogaira és szabadságaira nézve. Az új technológiák bevezetésének személyes és társadalmi következményei tehát beláthatatlanok lehetnek. Az adatvédelmi hatásvizsgálat révén az adatkezelő megismerheti és orvosolhatja az ilyen jellegű kockázatokat. Például bizonyos, a „dolgok internetét" használó alkalmazások jelentős hatást gyakorolhatnak az egyének mindennapi életére és magánéletére, ezért szükségessé teszik az adatvédelmi hatásvizsgálat elvégzését.

- Azok az esetek, amikor az adatkezelés önmagában véve „megakadályozza, hogy az érintettek a jogaikat gyakorolják vagy szolgáltatásokat vegyenek igénybe vagy szerződést érvényesítsenek"[GDPR rendelet 22. cikke és (91) preambulum bekezdése]. Ide tartoznak az érintettek számára szolgáltatás igénybevételének vagy szerződéskötésnek a lehetővé tételére, módosítására vagy elutasítására irányuló adatkezelési műveletek. Erre példa, ha egy bank hitelreferencia- adatbázis alapján szűri ügyfeleit, hogy eldöntse, kínál-e nekik hitelt.

Az esetek többségében az adatkezelő tekintheti úgy, hogy két szempontnak megfelelő adatkezelés esetében szükség van adatvédelmi hatásvizsgálatra.

4.5. A hatásvizsgálat mellőzésének esetei:

- ha az adatkezelés valószínűsíthetően nem jár „magas kockázattal [...] a természetes személyek jogaira és szabadságaira nézve" [GDPR rendelet 35. cikk (1) bekezdése];

- ha az adatkezelés a jellegét, hatókörét, körülményét és céljait tekintve nagyon hasonlít olyan adatkezelésre, amelyről már készült adatvédelmi hatásvizsgálat. Ilyen esetekben felhasználhatók a hasonló adatkezelés adatvédelmi hatásvizsgálatának eredményei [GDPR rendelet 35. cikk (1) bekezdése];

- ha az adatkezelési műveleteket felügyeleti hatóság meghatározott, azóta változatlan feltételek mellett 2018. május előtt ellenőrizte (lásd a GDPR rendelet III. fejezet C. szakaszát);

- ha a GDPR rendelet 6. cikk (1) bekezdés c) vagy e) pontja szerinti adatkezelési művelet jogalappal rendelkezik az uniós vagy tagállami jogban, a jog szabályozza az adott adatkezelési műveletet, és az említett jogalap megállapítása során már készült adatvédelmi hatásvizsgálat [GDPR rendelet 35. cikk (10) preambulum bekezdése], kivéve, ha a tagállam kimondta, hogy az adatkezelési műveletet megelőzően hatásvizsgálatot szükséges végezni;

- ha az adatkezelés szerepel azoknak az adatkezelési műveleteknek a (felügyeleti hatóság által összeállított) nem kötelező jegyzékében, amelyekre vonatkozóan nem kell adatvédelmi hatásvizsgálatot végezni.

5. A kockázatok kezelésére irányuló intézkedések:

Az azonosított kockázati tényezők kategorizálása után a következő lépés a kockázatokat csökkentő eljárások megfogalmazása, amelyek csökkentik vagy megszüntetik az adott kockázati tényezőt.

A kockázat kezelésére irányuló intézkedések bemutatása, ideértve a személyes adatok védelmét és a rendelettel való összhang igazolását szolgáló, az érintettek és más személyek jogait és jogos érdekeit figyelembe vevő garanciákat, biztonsági intézkedéseket és mechanizmusokat.

- Az adatbiztonság informatikai szempontú meghatározása.

6. Dokumentáció, azaz a kockázatelemzés összegzése, eredményének megállapítása:

Beszámoló elkészítése, a folyamat, a fennmaradó kockázatok leírása, gazdasági szempontú értékelése. Annak indoklással alátámasztott megállapítása, hogy szükséges-e az előzetes konzultáció.

7. Nyomon követés és felülvizsgálat:

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.

A kockázatok kezelésére hozott döntések rendszeres felülvizsgálatának a vezetési folyamat részévé kell válnia. Ezen túlmenően, az azonosítás - elemzés - értékelés - kezelésfolyamat (a kockázatok karaktereitől függő gyakoriságú) rendszeres ismétlése kritikus fontosságú az időbeli reagálás biztosítása miatt. A kockázatkezelési folyamatot magát, illetve eredményét (elemzés, döntéshozatal, ellenőrzés, kiegészítve a kontroll folyamatokkal) folyamatosan dokumentálni kell és gondoskodni kell a külső-belső érintettek megfelelő, rendszeres tájékoztatásáról is.

3. függelék

Adatlap az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény 28. § (2) bekezdése alapján az igénylő által megfizetendő költségtérítés teljesítéséhez szükséges személyes adatairól

Tájékoztatjuk, hogy az adatlapon található személyes adatait az adatkezelő számviteli bizonylat kiállításához használja fel. Az adatkezelés idejére és az adatok átadásának szabályaira a pénzügyi bizonylatok megőrzésére és ellenőrzésére vonatkozó törvényi előírások az irányadóak. Ennek megfelelően az adatokra vonatkozó adatkezelési idő 8 év.

Az adatkezelő a személyes adatokat harmadik fél számára csak külön törvényben foglaltak alapján megfelelő jogalap fennállása esetén adja át.

Az adatkezelő megnevezése: Borsod-Abaúj-Zemplén Vármegyei Katasztrófavédelmi Igazgatóság (a továbbiakban: BAZ VMKI)

Székhelye: 3525 Miskolc, Dózsa György út 15.

Postai címe: 3525 Miskolc, Dózsa György út 15.

Telefonszáma: (+36-46) 502-962

Adatvédelmi tisztviselője: dr. Polyák Zsolt tű. alezredes

Szolgálati helye: BAZ VMKI Hivatal

Elektronikus levélcíme: borsod.titkarsag@katved.gov.hu

Milyen jogok illetik meg az érintettet az adatkezelés kapcsán?

A tájékoztatáskéréshez való jog: az adatkezelőnél a tájékoztatóban felsorolt elérhetőségeken írásban tájékoztatást kérhet arról, hogy:

- milyen személyes adatait,

- milyen jogalapon,

- milyen adatkezelési cél miatt,

- milyen forrásból,

- mennyi ideig kezeli,

- az adatkezelő kinek, mikor, milyen jogszabály alapján, mely személyes adataihoz biztosított hozzáférést vagy kinek továbbította a személyes adatait,

- előfordult-e személyes adatai tekintetében adatvédelmi incidens.

Kérelmét az adatkezelő legfeljebb 30 napon belül, a megadott elérhetőségre küldött levélben teljesítjük.

A helyesbítéshez való jog: a tájékoztatóban felsorolt elérhetőségeken kérheti, hogy az adatkezelő módosítsa valamely személyes adatát (pl. hibásan feltüntetett képaláírás). Az adatkezelő a kérelmét legfeljebb 30 napon belül teljesíti, és erről a megadott elérhetőségre küldött levélben értesíti.

A törléshez való jog: a tájékoztatóban felsorolt elérhetőségeken kérheti az adatkezelőtől személyes adatainak törlését. Az adatkezelő az adattörlés iránti kérelem teljesítését abban az esetben tagadja meg, ha azokat jogszabály alapján kötelező kezelnie. Egyéb esetben a kérelmet legfeljebb 30 napon belül teljesíti, és erről a megadott elérhetőségre értesítést küld.

A korlátozáshoz való jog: a tájékoztatóban felsorolt elérhetőségeken küldött levélben kérheti személyes adatai kezelésének korlátozását. A korlátozás addig tart, amíg a megjelölt indok szükségessé teszi az adatok tárolását. Adatai kezelésének korlátozását kérheti például abban az esetben, ha úgy gondolja, hogy személyes adatait az adatkezelő jogellenesen kezelte, azonban az érintett által kezdeményezett hatósági vagy bírósági eljárás érdekében szükséges az, hogy az adatait, vagy az adatait tartalmazó dokumentumot az adatkezelő ne törölje. Ebben az esetben az adatkezelő a hatóság vagy a bíróság megkereséséig tovább tárolja a személyes adatot, majd a megkeresést és az adattovábbítást követően törli azt.

Mit tehet, ha úgy érzi, adatai kezelése kapcsán sérelem érte?

Amennyiben úgy érzi, hogy az adatkezelés során sérelem érte, kérjük, hogy elsődlegesen keresse meg az adatkezelő adatvédelmi tisztviselőjét a tájékoztatóban megjelölt elérhetőségeken.

Amennyiben az adatkezelő megkeresése nem vezetett eredményre, az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény 52. §-a alapján a Nemzeti Adatvédelmi és Információszabadság Hatóságnál bejelentést tehet, továbbá az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény 23. §-a, a Polgári Törvénykönyvről szóló 2013. évi V. törvény Második Könyv Harmadik Része, a polgári perrendtartásról szóló 2016. évi CXXX. törvény 502–503. §-a alapján bírósághoz fordulhat.

A Nemzeti Adatvédelmi és Információszabadság Hatóság elérhetősége:

Postacím: 1363 Budapest, Pf. 9

Telefon: +36 (1) 391-1400

Elektronikus postacím: ugyfelszolgalat@naih.hu

Honlap: www.naih.hu

A fenti tájékoztatást tudomásul veszem.

.....

Kelt: ..... év ..... hó ..... nap

A közérdekű adat megismerésére vonatkozó igény tárgya:

Az igénylő

Neve:

Címe:

Adóazonosító jele/adószáma:

Számlázásra vonatkozó adatok:

Számlázási név:

Számlázási cím:

Kelt: ..... év ..... hó ..... nap