

FŐVÁROSI
KATASZTRÓFAVÉDELMI
IGAZGATÓSÁG

FŐVÁROSI KATASZTRÓFAVÉDELMI IGAZGATÓ

20/2020. számú

INTÉZKEDÉSE

a Fővárosi Katasztrófavédelmi Igazgatóság Adatvédelmi, Adatbiztonsági és a közérdekű adatok nyilvánosságára vonatkozó Szabályzatának kiadásáról

Budapest, 2020. február 23-án.

A jogalkotásról szóló 2010. évi CXXX. törvény 23. § (4) bekezdés c) pontjának felhatalmazása alapján, az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény 25/A. § (3) és 30. § (6) bekezdéseire, valamint a hivatásos katasztrófavédelmi szervek adatvédelmi, adatbiztonsági és közérdekű adatok nyilvánosságára vonatkozó szabályzatáról szóló 4/2019. (VI. 20.) számú BM OKF utasításra tekintettel kiadom az alábbi

intézkedést:

1. Az intézkedés hatálya kiterjed a Fővárosi Katasztrófavédelmi Igazgatóság (a továbbiakban: FKI) minden szervezeti elemére és teljes személyi állományára.
2. Jelen intézkedés mellékleteként kiadom a Fővárosi Katasztrófavédelmi Igazgatóság Adatvédelmi, Adatbiztonsági és a közérdekű adatok nyilvánosságára vonatkozó Szabályzatát.
3. Ez az intézkedés a közzétételét követő napon lép hatályba.
4. Hatályát veszti a Fővárosi Katasztrófavédelmi Igazgatóság Adatvédelmi, Adatbiztonsági és a közérdekű adatok nyilvánosságára vonatkozó Szabályzatának kiadásáról szóló 5/2018. számú FKI igazgatói intézkedés.



Dr. Varga Ferenc tű. dandártábornok
igazgató

Készült: 1 eredeti példányban
Egy példány: 1 lap
Melléklet: 36 lap + 28 lap függelék
Készítette: dr. Cseh Zoltán
Kapja: Irattár

Jogi szempontból megfelelő:

..... (aláírás)
..... (név)
..... (dátum)

Melléklet a 10/2020. számú FKI igazgatói intézkedéshez

**A FŐVÁROSI KATASZTRÓFAVÉDELMI IGAZGATÓSÁG
ADATVÉDELMI, ADATBIZTONSÁGI ÉS A KÖZÉRDEKŰ
ADATOK NYILVÁNOSSÁGÁRA VONATKOZÓ
SZABÁLYZATA**

I. Fejezet

Általános rendelkezések

1. A szabályozás célja

1. A Fővárosi Katasztrófavédelmi Igazgatóság (a továbbiakban: FKI) adatvédelmi, adatbiztonsági és közérdekű adatok nyilvánosságára vonatkozó szabályzata (a továbbiakban: Szabályzat) kibocsátásának célja, hogy az Igazgatóság 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 az Igazgatóság kezelésében lévő közérdekű adatok nyilvánosságának biztosítása, ennek érdekében a közérdekű adatok megismerésére irányuló igények elbírálása, illetve az elektronikus formában közzeendő adatok megismerésére irányuló igények elbírálása során irányadó eljárási szabályok, valamint az elektronikus formában közzeendő adatok nyilvánosságra hozatalával összefüggő feladatok meghatározása.

2. Értelmező rendelkezések

2. Jelen szabályzat alkalmazása során:

2.1. **adatbiztonság:** a személyes adatok jogosulatlan kezelése, így különösen megszerzése, feldolgozása, megváltoztatása 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 a minimálisra csökkentik.

2.2. **adatfelelős szervezeti elem:** az FKI azon szervezeti eleme, amely az elektronikus úton kötelezően közzeendő közérdekű adatot előállította, illetve amelynek a működése során ez az adat keletkezett, vagy amely részére működése során az adatot szolgáltatták.

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

2.4. **adatközlő:** az FKI azon szervezeti eleme vagy az a személy, amely vagy aki az adatfelelős által hozzá eljuttatott adatokat a szerv közzétételi listáiban közzéteszi.

2.5. **dolgozói személyes adat:** az FKI-nál hivatásos szolgálati, igazgatási jogviszonyban, munkaviszonyban álló személyek, továbbá a közfoglalkoztatottak célhoz kötöttség elvének betartásával kezelt adata.

2.7. **ügyfélkapcsolati személyesadat-kezelés:** a hatósági ügyintézés körén kívül eső ügyfélkapcsolatokból, szerződéskötésekből származó személyes adatok kezelése a célhoz kötöttség elvének betartásával.

2.9. **nyilvántartási célú személyesadat-kezelés:** előre meghatározott szempontok alapján gyűjtött személyesadat-fajtákból adott szempontok szerint strukturált papíralapú vagy elektronikus adatállomány, amelyben az adatkezelés időtartama alatt biztosított az adatok különböző jellemzők alapján történő visszakereshetősége, lekérdezhetősége. Nyilvántartási célú adatkezelésnek minősül az is, amennyiben az adatok a nyilvántartás felvételét megelőző ügyfélkapcsolati, hatósági eljárásához kapcsolódó adatkezelésből származnak, de az adatok kezelése az adatkezelési cél tekintetében elválik az alapeljárástól.

2.10. ügyviteli célú személyes adat-kezelés: az FKI által a hatósági ügyek ellátása érdekében kezelt személyes adatok, ideértve a hatáskör gyakorlásához más adatkezelő által rendelkezésre bocsátott személyes adatokat is. Az ügyvitelhez kapcsolódó adatkezelés szorosan az ügy feldolgozásához kapcsolódik, alapvető célja az adott ügyhöz kapcsolódó eljárás lefolytatásához, az eljárás szereplőinek azonosításához és az ügy befejezéséhez szükséges adatok biztosítása. Az ügyviteli célú adatkezelés során a személyes adatok kizárólag az adott ügy irataiban szerepelnek, kezelésükre ezen célból csak az alapul szolgáló irat selejtezéséig van lehetőség.

2.11. adatkezelői tevékenységek nyilvántartása: az FKI személyes adatokra vonatkozó adatkezeléseit tartalmazó nyilvántartás, amelyet az adatvédelmi tisztviselő vezet.

2.12. közzétételi lista: az FKI által honlapon kötelezően nyilvánosságra hozott adattartalom, amely lehet:

a) **általános közzétételi lista:** az 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 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

Az adatvédelmi intézményrendszere

3. Az adatkezelések szintjei

3. A katasztrófavédelem 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 helyi adatkezelő szervek a katasztrófavédelmi kirendeltségek és a hivatásos tűzoltóságok.

4. Az adatkezelő szerv vezetőjének felelősségi rendszere

4. Az adatvédelemre és információszabadságra vonatkozó előírások alkalmazása során adatkezelő szerv vezetőjének kell tekinteni az FKI igazgatóját.

5. Az adatkezelő szerv vezetője felelős:

a) a vezetése 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) az alárendelt személyi állomány adatvédelmi oktatásáért és továbbképzéséért;

c) a vezetése vagy 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 naprakésztségéért;

d) az érintett törvényben meghatározott jogainak gyakorolásához szükséges feltételek biztosításáért.

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

7. Amennyiben a személyes adatokhoz való jog megsértése miatt az FKI-nak 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. Az adatkezelő szerv vezetőjének feladat- és hatásköre

8. Az FKI igazgatójának feladat- és hatásköre:

a) a jogszabály által a feladat- és hatáskörbe utalt adatkezelési rendszerek egészének (nyilvántartások, adattárak, munkafolyamatok, információáramlások és feldolgozások, jogosultságok) kialakítása és irányítása, rendeltetésszerű működtetése, melynek keretében teljes felelősséget visel a személyes adatok kezelésére vonatkozó törvények és az ezen alapuló rendelkezések érvényre juttatásáért;

b) gondoskodik a személyes adatok körében a jogosulatlan hozzáférés, közlés, megváltoztatás, vagy törlés megelőzéséről, a 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 való jogát;

c) személyes felelősséggel tartozik az általa vezetett szerv, illetve irányítása alá tartozó szervek tevékenységéért, azok törvényes és szakszerű működéséért, ezen belül az irányítása alatt álló állomány adatkezelői tevékenységéért, az adatvédelmi előírások, valamint a kapcsolódó ügyviteli és minősítettadat-védelmi szabályok betartásáért;

d) a védelmi és biztonsági szabályok gyakorlati érvényesülésének ellenőrzése, intézkedés a hiányosságok felszámolására;

e) az adatkezelések szervezeti és működési feltételeinek kialakítása, gondoskodás a működési követelmények és az adatbiztonsági követelmények érvényre juttatásáról;

f) az adatszolgáltatásokról vezetett nyilvántartás ellenőrzése.

6. A területi szervek adatvédelmi tisztviselői

9. Az FKI igazgatója köteles az irányítása alá tartozó személyi állományból az adatvédelmi tevékenység irányítása, felügyelete és ellenőrzése érdekében - jogi, közigazgatási, informatikai, vagy ezeknek megfelelő felsőfokú végzettséggel rendelkező - területi adatvédelmi tisztviselőt kijelölni, aki egyéb feladatokkal csak az adatvédelmi feladatok ellátásának veszélye nélkül bízható meg.

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

11. A területi adatvédelmi tisztviselő feladata:

- a) segíti az FKI igazgatóját és a helyi adatvédelmi tisztviselőt a katasztrófavédelmi adatkezelésre vonatkozó jogszabályok és belső normák érvényre juttatásában, figyelemmel kíséri az adatvédelemmel összefüggő jogszabályváltozásokat, előkészíti az adatkezelő szerv vezetőjének adatvédelmi tárgyú döntéseit;
- b) vizsgálja 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 FKI igazgatójának megbízásából ellenőrzi az Igazgatóságnál 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 az FKI igazgatójánál kezdeményezi a felelősség megállapításához szükséges eljárás lefolytatását;
- e) gondoskodik az FKI személyi állománya és a helyi adatvédelmi tisztviselők oktatásáról, szükség szerinti vizsgáztatásáról, a helyi szerv személyi állományának oktatásához segédanyagot biztosít a helyi adatvédelmi tisztviselő részére vagy az oktatást ő maga végzi;
- f) elkészíti az FKI 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 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 az FKI honlapján megjelenített Adatvédelmi Irányelvek és adatkezelési tájékoztató naprakészen tartásáról;
- j) rendszeresen ellenőrzi az FKI közzétételi listáinak naprakészségét és teljességét;
- k) felügyeli az FKI 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 február 28-ig jelentésben értékeli az FKI adatvédelmi és adatbiztonsági helyzetét;
- n) végzi a személyes adatok kezelése és feldolgozása kapcsán tájékoztatás iránt benyújtott elutasított kérelmekkel, továbbá az elutasított közérdekűadat-megismerési igényekkel kapcsolatos tájékoztatást;
- o) ellátja az Egységes Közadatkereső Rendszerrel, valamint a Központi Jegyzékkel kapcsolatos, jogszabályban meghatározott feladatokat;
- p) amennyiben az adatvédelmi tisztviselő egyben jogtanácsos, a peres képviseletet ellátja adatvédelmi tárgyú perekben. Amennyiben az adatvédelmi tisztviselő és a jogtanácsos nem egy személy, az adatvédelmi tisztviselő közreműködik az adatvédelmi tárgyú perben, szakmai véleményével segíti a jogtanácsos perképviseletét, amennyiben jogász végzettséggel rendelkezik, a képviseletet az adatvédelmi tisztviselővel együtt látja el, egyébként a tárgyalásokon hallgatóságként részt vesz;
- q) ellátja mindazon feladatokat, amelyeket az FKI Adatvédelmi és Adatbiztonsági Szabályzata részére feladatként meghatároz.

12. A 11. m) pontban meghatározott jelentés tartalmazza különösen:

- a) az adatkezelő szervezeti elemeknél végzett adatvédelmi tárgyú ellenőrzések megjelölését, azok fontosabb megállapításait, a feltárt lényeges szabálytalanságokat, hiányosságokat, a megszüntetésükre tett intézkedéseket;
- b) az elvégzett honlapellenőrzések időpontját, eredményét és a hiányosságok pótlására vonatkozó információkat;
- c) az adatkezelő szervezeti elemek állományába tartozók ellen az adatvédelmi előírások megsértése miatt indított fegyelmi, szabálysértési és büntetőeljárásokra vonatkozó adatokat (az érintettek megjelölése nélkül);
- d) az adatkezelő szervezeti elemeknél 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 közzétételével biztosított helyzetét az FKI-nál, ideértve a NAIH felé küldött éves tájékoztató megtörténtét;
- h) az adatvédelem és információszabadság területén adódott egyedi ügyeket;
- i) a következő naptári évre tervezett feladatokat.

7. A helyi szervek adatvédelmi tisztviselői

13. Az FKI igazgatójának döntése alapján a helyi és területi adatvédelmi feladatok, valamint a területi adatvédelmi tisztviselő és a helyi adatvédelmi tisztviselő személye egymástól elkülönül.

14. Az FKI igazgatója – a kirendeltség-vezetők javaslatának figyelembe vételével – írásban jelöli ki a jogszabályban meghatározott feltételek szerint a helyi szintekre a helyi adatvédelmi tisztviselőket (Katasztrófavédelmi Kirendeltségenként 1 főt).

15. A helyi adatvédelmi tisztviselőnek jogi, közigazgatási, informatikai, vagy ezeknek megfelelő felsőfokú végzettséggel kell rendelkeznie. Amennyiben a helyi szerv személyi állományában nem áll rendelkezésre a helyi adatvédelmi tisztviselői feladatok ellátásához szükséges végzettséggel rendelkező személy, a feladatra olyan állománytagot kell kijelölni, aki munkaköréből, ismereteiből adódóan arra a legalkalmasabb.

16. A helyi adatvédelmi tisztviselő

- a) eljár a részére átruházott - és munkaköri leírásában rögzített - adatvédelemmel összefüggő feladatkörökben, így végzi:
 - aa) a felszerelők adatvédelmi tájékoztatását;
 - ab) az állománytagok nyilatkoztatását a kép- vagy kép- és hangfelvételen történő szereplésükhöz való hozzájárulásról;
 - ac) az adatvédelmi incidensekről szóló jelentések továbbítását a területi adatvédelmi tisztviselőnek;
 - ad) az adatvédelmi tárgyú (különösen a nyilvántartásokkal, a közérdekű adatigényekkel és a közzétételi listákkal kapcsolatos) feladatszabások végrehajtását;
 - ae) az adatvédelmi és adatbiztonsági szabályok betartását folyamatos ellenőrzését;
 - af) az adatvédelmi jogszabályváltozásokat nyomon követve, szervezi és megtartja – szükség esetén a területi adatvédelmi tisztviselő bevonásával – a helyi szintű továbbképzéseket.
- b) intézi az FKI igazgatójának utasítása, és az FKI területi adatvédelmi tisztviselőjének feladatszabása szerinti teendőket.

Az FKI igazgatója ugyanakkor továbbra is felelős az adatkezelés jogszerűsége érdekében a hatáskörébe tartozó intézkedések megtételéért.

III. Fejezet

A személyes adatok védelme

8. Az adatkezelés alapvető szabályai

17. Az FKI-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.

18. Az adatkezelő köteles az adatkezelési műveleteket úgy megtervezni és végrehajtani, hogy az Infotv.-ben és a Szabályzatban foglaltak alkalmazása során biztosítsa az érintettek magánszférájának védelmét.

19. 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.

20. 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 rendelkezhetőek.

21. A személyes adatok automatizált feldolgozása során az adatkezelő és az adatfeldolgozó további intézkedésekkel biztosítja:

- a) a jogosulatlan adatbevitel megakadályozását;
- b) az automatikus adatfeldolgozó rendszerek jogosulatlan személyek általi, adatátviteli berendezés segítségével történő használatának megakadályozását;
- c) annak ellenőrizhetőségét és megállapíthatóságát, hogy a személyes adatokat adatátviteli berendezés alkalmazásával mely szerveknek továbbították vagy továbbíthatják;
- d) annak ellenőrizhetőségét és megállapíthatóságát, hogy mely személyes adatokat, mikor és ki vitte be az automatikus adatfeldolgozó rendszerekbe;
- e) a telepített rendszerek üzemzavar esetén történő helyreállíthatóságát, és
- f) az automatizált feldolgozás során fellépő hibákról jelentés készítését.

22. 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.

23. 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 Iratkezelési Szabályzatában és az Informatikai Biztonsági Szabályzatban foglaltak ismeretéből az adatvédelmi tisztviselő és az ügykezelésért felelős vezető által szervezett 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.

9. Adatkezelések fajtái, adatkezelések megkezdése, adatvédelmi hatásvizsgálat, az érintetti jogok

24. Az FKI adatkezelése törvényi felhatalmazáson vagy az érintett hozzájárulásán, dolgozói adatkezelések tekintetében a munkáltató adatkezelői érdekén, az érintett által igényelt juttatások esetén az érintett vélelmezett hozzájárulásán alapulhat.

25. Amennyiben a személyesadat-kezelést nem törvény rendeli el, az adatfelvételt belső szabályozóval vagy egyéb írásos formában kell elrendelni. Erre az FKI igazgatója, helyi szintű adatkezelés esetén a katasztrófavédelmi kirendeltség vezetője jogosult.

26. 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, akkor előzetes hatásvizsgálatot végez arra vonatkozóan, hogy a tervezett adatkezelési műveletek a személyes adatok védelmét hogyan érintik.

27. 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.

28. Az adatvédelmi hatásvizsgálat szükségességének megállapításához az érintett szakterület megválaszolja az *1. számú függelékben* foglalt kérdéseket.

29. 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.

30. 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 FKI igazgatójánál.

31. Az FKI igazgatója 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.

32. 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.

33. Az adatkezelési hatásvizsgálatot végző szakterület az adatvédelmi hatásvizsgálatról összefoglaló jelentést készít a *2. számú függelék* alapján. Az összefoglaló jelentést az FKI igazgatója hagyja jóvá, amelyet követően az adatkezelést a 25. pont szerint kell elrendelni.

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

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

36. 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 való jog) jog tájékoztatáskérési, helyesbítési és törléskezdeményezési, valamint tiltakozási jog)és azokat milyen módon érvényesítheti;
- e) az adatvédelmi tisztviselő nevééről és elérhetőségéről;
- f) milyen jogorvoslati lehetőséggel rendelkezik (NAIH-hoz fordulás, bírósági jogérvényesítés útja).

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

38. Az egyedi ügyekben alkalmazandó hozzájáruló nyilatkozatot, valamint az ahhoz tartozó adatvédelmi tájékoztatót az FKI helyi adatvédelmi tisztviselője, a rendszeresen előforduló, adatkezelési hozzájárulást igénylő ügyekben alkalmazandó hozzájáruló nyilatkozatot az FKI területi adatvédelmi tisztviselője az érintett szakterület közreműködésével készíti el.

39. 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.

40. A hivatásos katasztrófavédelmi szervek - az adatkezelés eltérő célja alapján - ügyviteli, ügyfélkapcsolati, dolgozói, illetve nyilvántartási célú (adatállomány kialakítására irányuló) adatkezelést végeznek.

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

10. Adatvédelmi incidensek nyilvántartása

42. Aki a tevékenységének ellátása során az FKI által végzett adatkezeléssel kapcsolatban adatvédelmi incidens bekövetkezését észleli, köteles azt a szolgálati út betartásával jelezni az FKI helyi vagy területi adatvédelmi tisztviselőjének.

43. Aki a munkáltató által végzett adatkezelés kapcsán saját személyes adatai tekintetében adatvédelmi incidens bekövetkezését észleli, jogosult azt közvetlenül jelezni az FKI területi adatvédelmi tisztviselőjének.

44. Az FKI területi adatvédelmi tisztviselője a 42-43. pont alapján 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.

45. A bekövetkezett adatvédelmi incidensek tekintetében a következmények elhárítási és a hasonló esetek bekövetkezésének megelőzési módjára az FKI területi adatvédelmi tisztviselője tesz javaslatot.

11. Személyes adatot tartalmazó nyilvántartások kialakítására vonatkozó rendelkezések

46. Nyilvántartási célú személyesadat-kezelés végzése céljából nyilvántartás törvény vagy törvényi felhatalmazás alapján hozható létre. A nyilvántartás vezetésére ily módon jogosított vagy kötelezett adatkezelő által végzett adatkezelés technikai részletei szabályozhatók egyéb jogszabályban vagy belső szabályozóban.

47. Amennyiben a nyilvántartás kialakítását nem törvény rendeli el, létrehozatalát belső szabályozóval vagy egyéb írásos formában kell elrendelni. Erre területi szintű adatkezelés esetén az FKI igazgatója, helyi szintű adatkezelés esetén a katasztrófavédelmi kirendeltség vezetője jogosult. Az így létrehozott nyilvántartásba személyes adat kizárólag az érintett dokumentált hozzájárulásával vihető be.

48. A nyilvántartásban kezelt adatok körét és kezelési időtartamát az adatkezelésre jogosító vagy kötelező jogszabály vagy az érintett hozzájárulásában foglaltak határozzák meg.

49. A törvény alapján létrehozandó nyilvántartás felvételéről a hivatásos katasztrófavédelmi szerv területi adatvédelmi tisztviselőjét haladéktalanul értesíteni kell.

50. Nyilvántartási kötelezettséget előíró belső szabályozó vagy írásbeli döntés előkészítése során be kell szerezni – döntési szinttől függően – a helyi vagy a területi adatvédelmi tisztviselő véleményét.

51. A megkeresésben a tervezett nyilvántartás vonatkozásában meg kell határozni:

- a) az adatkezelésért felelős szervezeti elemet,
- b) az adatkezelés tényleges fizikai helyét,
- c) az adatkezelés jogalapját,
- d) az adatkezelés pontos célját,
- e) az adatfelvétel módját,
- f) az érintettek körét,
- g) az adatállományt kezelő informatikai rendszer megnevezését, feladatait,
- h) amennyiben van kapcsolat más szervek adatállományaival, ezen adatállományok megjelölését,

- i) amennyiben az adatállományból lehetséges adattovábbítás, annak jogalapját, feltételeit, címzettjét,
- j) az adatok informatikai biztonsági és adatvédelmi-adatbiztonsági minősítését, megőrzési, megsemmisítési szabályait,
- k) az adatállomány naprakészességét biztosító módszert.

52. A nyilvántartások kizárólag a létrehozatalukat szolgáló cél érdekében, a cél eléréséhez szükséges mértékben és ideig tartalmazhatnak adatokat, a nyilvántartásban található adatok a nyilvántartásától eltérő célra törvényi felhatalmazás vagy érintetti hozzájárulás hiányában nem felhasználhatóak.

53. A nyilvántartás kezelője köteles gondoskodni az adatok pontosságáról, naprakészességéről, az adatkezelés célját már nem szolgáló adatok törléséről. Amennyiben a nyilvántartás vezetője a helyi adatvédelmi tisztviselő, úgy erről írásban tájékoztatja a területi adatvédelmi tisztviselőt.

12. A adatkezelői tevékenységek nyilvántartása

54. Az FKI területi adatvédelmi tisztviselője legkésőbb az adatkezelés megkezdése előtti tizennegyedik napig köteles a kezelésében lévő személyes adatokkal kapcsolatos adatkezeléseiről vezetett nyilvántartásban legalább az alábbi adatkezelési adatokat rögzíteni:

- a) az adatkezelés célját,
- b) az adatkezelés jogalapját,
- c) az érintettek körét,
- d) az érintettekre vonatkozó adatok leírását,
- e) az adatok forrását,
- f) az adatok kezelésének időtartamát,
- g) amennyiben az adattovábbítás elvi lehetősége fennáll, a továbbítható adatok fajtáját, címzettjét és a továbbítás jogalapját, ideértve a harmadik országokba irányuló adattovábbításokat is;
- h) a tényleges adatkezelés helyét (a szervezeti elem és az adatok fizikai helyének megjelölésével),
- i) ha az adatkezelő adatfeldolgozót vesz igénybe, az adatfeldolgozó nevét és címét vagy székhelyét, az adatfeldolgozás helyét és az adatfeldolgozónak az adatkezeléssel összefüggő tevékenységét, az alkalmazott adatfeldolgozási technológia jellegét.

55. Az adatkezelésekben bekövetkezett változást vagy az adatkezelés megszüntetését a bejelentésre kötelezett nyolc napon belül bejelenti az FKI területi adatvédelmi tisztviselőnek.

13. Az adatfeldolgozás szabályai

56. Az FKI igazgatójának döntése alapján az Igazgatóság adatfeldolgozót vehet igénybe.

57. Az adatfeldolgozásra vonatkozó szerződést írásba kell foglalni, amely 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
- k) az adatkezelő részére nyújtott, az érintettek jogainak érvényesítésében való segítségnyújtási és az adatkezelő részére történő információátadási kötelezettséget.

14. Közös adatkezelés szabályai

58. Amennyiben ugyanazon személyes adatokat ugyanazon adatkezelési jogalap és cél alapján több hivatásos katasztrófavédelmi szerv kezel, az adatkezelés szabályait megállapodásban rögzítik, különös tekintettel:

- a) az érintettek tájékoztatására vonatkozó kötelezettségre,
- b) az érintetti jogok gyakorlásának biztosítására,
- c) az adatvédelmi incidensek kezelésére,
- d) az adattovábbítások dokumentálására,
- e) az adatkezeléssel kapcsolatos felelősségi kérdésekre.

15. Adattovábbítás az FKI adatkezeléséből

59. Az FKI adatkezeléséből személyes adatot továbbítani az érintett hozzájárulásának hiányában csak törvényben meghatározott szerv vagy személy részére, törvényben meghatározott adatkörben lehet, a célhoz kötöttség elvének maradéktalan érvényesítésével.

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

61. Az adattovábbítás 59-60. pontban meghatározott feltételeinek meglétét az adatot továbbító adatkezelő minden egyes személyes adattal összefüggésben ellenőrizni köteles.

62. Harmadik személy vagy szerv által benyújtott adattovábbítási kérelem elbírálása - a törvényben kötelezően előírt adattovábbítás esetét kivéve - az FKI igazgatójának, vagy az általa kijelölt vezetőnek a hatáskörébe tartozik. Az adatigénylést abban az esetben teljesítheti, ha az tartalmazza:

- a) az adatigénylés célját, jogalapját (az alapul szolgáló törvényi rendelkezés pontos megjelölését);
- b) a kért adatok körének pontos meghatározását;
- c) az érintett személy azonosításához szükséges adatokat, több személyre vonatkozó adatigénylés esetén az érintettek azonosításához szükséges csoportképző ismérveket.

63. Az FKI - törvény eltérő rendelkezése hiányában - csak olyan személyes adatokat továbbíthat, amelyeknek az Igazgatóság az Infotv.-ben meghatározott 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.

64. 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.

65. Az Európai Unió vagy más külföldi projektekből és az államháztartás alrendszereiből nyújtott támogatásokkal történő elszámolások elkészítése során az elszámoláshoz szükséges személyes adatokat a projekttel vagy a támogatással kapcsolatos feladatokban részt vevő állománytagokkal az *5. számú függelékben* található Adatkezelési Tájékoztatót és Hozzájáruló Nyilatkozatot alá kell íratni.

16. A közvetlen lekérdezés

66. A közvetlen lekérdezés lehetőségének megteremtésére irányuló kérelmet az FKI igazgatója - az érintett szakmai és informatikai szakterület 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.

67. 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.

68. 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.

69. A lekérdezési lehetőség biztosítása esetén az FKI igazgatója felelős azért, hogy a lekérdezett adatokhoz csak az arra jogosultak férhetnek hozzá. Az adatigénylő részéről lekérdezésre feljogosított személy felelős azért, hogy kizárólag az engedélyezett célra és az engedélyben meghatározott adatokat kérje le, valamint a lekérdezett adatokat csak jogszerű - az engedélyben meghatározott - célra használja fel.

70. Az adatigénylő szerv a lekérdezésre jogosult személyekről és egyedi azonosítójukról köteles naprakész nyilvántartást vezetni. A jogosultak személyéről és az abban bekövetkezett változásokról az adatkezelő szervet kérésére - illetve a megállapodásban vagy a szerződésben meghatározott esetekben - tájékoztatni kell.

71. 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 jogosultak a visszaélések megakadályozása érdekében jelszavukat más személynek nem hozhatják tudomására.

72. 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 a lekérdezést végző maga köteles dokumentálni az érintett adatkezelés megjelölését, az adatlekérdezés időpontját és célját.

17. Adattovábbítás hírközlő eszköz alkalmazásával

73. Az FKI 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.

74. 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.

75. 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 (a 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.

18. Az adatigénylés során irányadó szabályok

76. Az FKI adatállományokból 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.

77. 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.

78. 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.

79. 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 (a 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.

80. 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.

19. Az érintetti jogok gyakorlása

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

82. Az FKI-nál az érintetti jogok gyakorlása tekintetében az érintettekkel a területi adatvédelmi tisztviselő tartja a kapcsolatot, kivéve, ha az adott jog és az adott adatkezelés tekintetében a szakterülettel történő közvetlen kapcsolattartás indokolt.

83. A beérkezett kérelmeket a területi adatvédelmi tisztviselő továbbítja az adatkezelést végző szervezeti elem részére.

84. Az érintettet megillető jogok gyakorlására csak az érintett kérelmező megfelelő azonosítása esetén van lehetőség. Az érintett kérelmező személyének azonosításához a természetes személyazonosító adatok ellenőrzése szükséges.

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

86. A beérkezett kérelmeket az adatkezelő legfeljebb 25 napon belül, a megadott elérhetőségre küldött levélben teljesíti.

87. Az adatkezelő az adattörlés iránti kérelem teljesítését abban az esetben tagadja meg, ha azokat jogszabály alapján kötelező kezelnie. Egyéb esetben a 86. pont szerint teljesíti.

88. 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.

89. Az adat helyesbítéséről vagy törléséről 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, a területi adatvédelmi tisztviselőt a levél másolatának megküldésével tájékoztatják.

90. Az érintett hozzáférési jogának gyakorlása során az adatkezelő az érintett jogainak ismételt és megalapozatlan érvényesítésével összefüggésben közvetlenül felmerült költségeinek megtérítését az FKI-hoz érkezett közérdekűadat-megismerési igények teljesítésével kapcsolatos költségtérítés összegének meghatározása során alkalmazandó önköltségszámítási szabályok szerint követelheti az érintettől.

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

20. Eljárás a NAIH fellépése esetén

92. Amennyiben az FKI-nál a NAIH

- a) vizsgálatot,
- b) adatvédelmi hatósági eljárást, vagy
- c) titokfelügyeleti hatósági eljárást

indít, a területi adatvédelmi tisztviselő a BM OKF adatvédelmi tisztviselőjét - a szolgálati út betartásával - haladéktalanul értesíti.

93. A NAIH vizsgálatával, valamint az adatvédelmi és a titokfelügyeleti hatósági eljárással érintett adatkezelő szervezeti elem 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.

94. Az adatkezelő a 93. pontban meghatározott kötelezettségeinek az Infotv. 54. § (2) bekezdésében meghatározott határidőig köteles eleget tenni.

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

96. Az FKI 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) bekezdésben foglaltak szerint jár el.

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

98. 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

Az FKI-nál folytatott egyes adatkezelések

21. Az FKI személyi állományába tartozó személyek adatainak kezelése

99. Az FKI személyi állományába tartozó személyek személyes és különleges adatainak kezelését - ideértve a közszolgálati adatvédelmi szabályzatra vonatkozó előírásokat - a mindenkor hatályos Humán Szabályzat szabályozza, amely különösen az alábbiakról rendelkezik:

- a) a dolgozói adatkezelésben résztvevő szervek és személyek általános adatvédelmi kötelezettségei,
- b) az adatkezelők és felhasználók felelőssége,
- c) a kezelésbe vonható személyes és különleges adatok köre,
- d) betekintés a személyügyi nyilvántartásba,
- e) a személyi állomány adatszolgáltatási kötelezettsége,
- f) a saját személyes adatok megismerése,
- g) a betekintés menete és a betekintési lap alkalmazásának szabályai,
- h) tájékoztatás személyes adatokról,
- i) az egészségügyi adatok kezelésére vonatkozó előírások,
- j) a vagyonyilatkozattal kapcsolatos adatok kezelése,
- k) a személyi iratok és a személyes adatokat tartalmazó adathordozók fizikai védelme,
- l) személyes adatokat tartalmazó számítógépes információs rendszer adatvédelme és adatbiztonsága.

100. A hivatásos katasztrófavédelmi szervek közötti olyan ügyintézés során, amikor dolgozói személyes adatok továbbítására kerül sor, az iratokat minden esetben zárt borítékban, az adatkezelő szervezeti egység megjelölésével és a borítékban lévő adatok típusának megjelölésével szükséges küldeni. A borítékon kerüljön feltüntetésre, hogy „Személyes adatot tartalmaz, felbontás szervezeti egység által.”

22. Az FKI személyi állományába jelentkezők személyes adatainak kezelése, az új belépők tájékoztatása

101. Az FKI által meghirdetett álláshelyekre benyújtandó pályázatok kötelező tartalmi elemeként elő kell írni adatkezelési hozzájárulás benyújtását. Az álláshely meghirdetések az adatkezelési tájékoztatásra vonatkozó általános szabályok szerint tájékoztatni kell a lehetséges pályázókat az adatkezelés körülményeiről.

102. Annak érdekében, hogy a nem pályázati kiírás eredményeként érkező önéletrajz benyújtója személyes adatok védelméhez fűződő joga ne sérüljön, az FKI honlapján az önéletrajzok kezelésével és tárolásával kapcsolatos tájékoztatót kell elhelyezni az Állaspályázatok link alatt, melyben fel kell hívni a figyelmet arra, hogy az érintettek a beküldött önéletrajzához csatolnia kell egy nyilatkozatot, amelyben hozzájárul önéletrajzának 3 hónapig tartó kezeléséhez. Amennyiben a beérkezett nyilatkozat a hozzájárulást nem tartalmazza, a hivatásos katasztrófavédelmi szerv 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.

103. 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.

104. 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.

105. Az FKI területi adatvédelmi tisztviselője a szerv által végzett dolgozói adatkezelésekről tájékoztatót készít, amelyet a helyi adatvédelmi tisztviselők az új állománytagok részére a munkába állást követően átadnak. Az új állománytag az ismeretek átadását aláírásával igazolja, a törvényben meghatározott, kötelező hozzájárulást megadja.

23. Alkalmassági vizsgálatok

106. Az egészségügyi, pszichológiai és fizikai alkalmassági vizsgálat elrendelésével egyidejűleg tájékoztatni kell az érintetteket:

- a) a vizsgálat elrendelését előíró jogszabályokról,
- b) a vizsgálat céljáról - az egészségügyi és pszichológiai alkalmassági vizsgálat esetén lehetőség szerint kitérve az egyes részvizsgálatok céljára is,
- c) az adatok megőrzési idejéről,
- d) az adatkezelést végző személyéről,
- e) arról, hogy az adatok továbbíthatóak-e és
- f) az érintett vizsgálati eredményekbe történő betekintési, valamint jogorvoslati jogáról.

107. A tájékoztatás történhet az érintettnek a hivatásos állományba kerülést vagy az első alkalmassági vizsgálatot megelőzően átadandó űrlapon történő adatvédelmi tájékoztató feltüntetésével is, ilyenkor az érintettnek az űrlapon jeleznie kell, hogy a tájékoztatóban foglaltakat tudomásul vette.

24. Telefon- és internethasználat ellenőrzése

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

109. A vezetékess munkahelyi telefonok használatával kapcsolatos adatvédelmi kérdéseket a BM Országos Katasztrófavédelmi Főigazgatóság Informatikai Szakterületének Gazdálkodási Szabályzatáról szóló főigazgatói intézkedés rendezi.

25. A hivatásos katasztrófavédelmi szervek személyi állományáról készült képfelvételekkel kapcsolatos adatkezelés

110. Az FKI személyi állományáról készült 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 a *3. számú függelék* szerinti nyilatkozat kitöltésével kell megszerezni, kivéve, ha a felvétel:

- a) nyilvános közéleti szereplés során készült felvételnek minősül,
- b) tömegfelvételnek minősül,
- c) ha a felvétel a hivatásos állomány tagjáról technikai ellenőrzés keretében, a térfelügyelő kamerákra vonatkozó rendelkezés szerint a szolgálatellátás ellenőrzése céljából vagy
- d) az ellátott szolgálati feladattal összefüggésben hatósági ellenőrzés vagy beavatkozás során készül.

111. A hozzájáruló nyilatkozat aláírása önkéntes. Azon állománytagok nevét, akik nem kívánnak a felvételeken szerepelni, e joguk érvényesítése érdekében - nevet, rendfokozatot, beosztást, vonulós állomány esetén a szolgálati csoportot is megjelölve - nyilvántartásba kell venni.

112. A hozzájáruló nyilatkozatokat a helyi adatvédelmi tisztviselők összegyűjtik, a nyilvántartást elkészítik, majd megküldik a területi adatvédelmi tisztviselőnek, aki átadja a kép- vagy kép- és hangfelvételeket készítő személyekkel napi munkakapcsolatban álló szövegíróknak. A nyilvántartott neveket kizárólag a felvételekkel kapcsolatos adatkezelést végző személyek, valamint az adatvédelmi tisztviselő ismerheti meg.

113. A hozzájáruló nyilatkozatokat a területi adatvédelmi tisztviselő zárható szekrényben kezeli.

114. Rendezvényen történő kép- és hangfelvétel készítése esetén a rendezvényért felelős szervezeti elem feladata a rendezvény megkezdése előtt felhívni az érintettek figyelmét arra, hogy amennyiben a képfelvétel készítéséhez - ide nem értve a tömegfelvételt és a nyilvános közéleti szereplést - nem járulnak hozzá, úgy azt jelezzék a jelenlévő fotós részére.

115. A jelenléti vagy regisztrációs ív alkalmazásával járó események esetén az adatkezelési tájékoztatót jól látható helyen elérhetővé kell tenni, és a jelenléti íven vagy regisztrációs adatlapon az adatkezelési hozzájárulásnak külön rubrikát kell kialakítani.

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

116. Az FKI 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 a *4. számú függelék* szerinti nyilatkozat kitöltésével kell megszerezni, kivéve, ha a felvétel:

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

- c) az FKI által ellátott szolgálati feladattal összefüggésben hatósági ellenőrzés vagy beavatkozás során készül.

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

118. 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 vagy területi jogállású szervek honlapja, Médiaszerver, Facebook-oldal, Katasztrófavédelem elektronikus magazin, Szent Flórián Önkéntestűzoltóportál) kiterjedjen.

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

120. A 114. és 115. pontban foglaltakat a nem az FKI állományába tartozó személyeket is érintő rendezvények esetén szintén alkalmazni kell.

27. Képfelvevők telepítése a hivatásos katasztrófavédelmi szervek objektumaiban, készenléti járművein

121. Az FKI épületein, objektumain és objektumaiban és az azokhoz tartozó magánterületen, közönség számára nyilvános magánterületen, - így különösen parkolóban -, valamint készenléti járműveken képfelvevő telepítése esetén az új személyesadat-kezelés megkezdésére vonatkozó szabályokat kell megfelelően alkalmazni.

122. Nem alkalmazható elektronikus megfigyelőrendszer vagy technikai ellenőrzésre szolgáló más eszköz olyan helyen, ahol a megfigyelés az emberi méltóságot sértheti, így különösen öltözőben, mosdóban, illemhelyen, egészségügyi vagy pszichológiai vizsgálat céljára szolgáló helyiségben, ideértve a vizsgálati helyiséghez tartozó váróhelyiséget is.

123. Még technikai ellenőrzéssel összefüggően sem helyezhető el a munkavégzés, munkahelyi viselkedés megfigyelése céljából kamera olyan helyiségekben, ahol állandó munkavégzés folyik, sem pedig a munkaközi pihenés céljából szolgáló helyiségekben, kijelölt dohányzóhelyen, ügyeleti helyiségben.

124. A fenti rendelkezések alól kivételt képeznek az olyan munkahelyiségek, ahol az állománytagok élete, testi épsége veszélyben lehet, így pl. kivételesen működtethető kamera szerelőcsarnokban vagy más veszélyforrást tartalmazó objektumban.

125. Az FKI jelentős értéket képező eszközök - így különösen a szerek - elhelyezéséről szolgáló helyiségeiben, így különösen garázsban, egyéb, jelentős értéket képviselő eszközök tárolására szolgáló raktárban és az azokhoz vezető folyosókon, készenléti járműveken elhelyezhető és működtethető képfelvevő, azok működéséről azonban jól látható helyen és módon tájékoztatni kell az érintetteket. Olyan időszakban és épületrészekben, amikor és ahol fő szabály szerint senki nem tartózkodhat, vagyonvédelmi célból szintén elhelyezhető képfelvevő.

126. A képfelvevő által rögzített kép-, hang-, valamint kép- és hangfelvételt felhasználás hiányában legfeljebb a rögzítéstől számított 30 munkanap elteltével meg kell semmisíteni, illetve törölni kell, a technikai ellenőrzés keretében készített felvételek kivételével.

127. A képfelvevők telepítése abban az esetben felel meg az adatvédelmi követelményeknek, amennyiben a képfelvevő által megfigyelt területre belépő személy számára jól látható módon elhelyezésre kerül a „Kamerával megfigyelt terület” figyelmeztetés.

128. A képfelvevők által vett képet közvetítő berendezést úgy kell elhelyezni, hogy azt csak az a személy láthassa, akinek a képfelvevő által közvetített kép figyelése a szolgálati feladatainak részét képezi.

129. A képfelvevőkkel kapcsolatos adatkezelés dokumentálása érdekében betekintési naplót is rendszeresíteni kell, amely a felvételekbe történő valamennyi betekintés vonatkozásában tartalmazza a betekintő megnevezését, a betekintés okát, jogalapját, dátumát.

28. Mozgó kamerák

130. A gépjárműben felszerelésre kerülő kamerának az alábbi általános műszaki feltételeknek kell megfelelnie:

- a) nagylátószögű (legalább 120 fokos) rögzítést tegyen lehetővé;
- b) a kamera által rögzített állomány utólag - az anonimizálástól eltekintve - ne legyen manipulálható;
- c) beépített GPS helymeghatározó legyen a készülékben;
- d) a rögzített felvételen látszódjon a pontos idő, a gépjármű sebessége, valamint a GPS koordináták is;
- e) beépített G-sensorral, Black-box funkcióval, (karambol, borulás stb. érzékelése) rendelkezzen;
- f) ciklikus rögzítésű legyen, automata kikapcsolással és automata bekapcsolással rendelkezzen;
- h) Motion Detection mozgásérzékelő funkcióval rendelkezzen (a lencse előtt történő mozgás hatására a felvétel elinduljon).

131. 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 az FKI később fel kívánja használni, de a felhasználási cél az arcképek kezelését nem indokolja, olyan technikai háttérrel kell biztosítani, amely alkalmas a személyazonosításra alkalmas felvételek anonimizálására.

132. 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.

133. Az FKI gépjárművébe a szolgálatteljesítést ellenőrző technikai eszközként telepített képfelvevő által rögzített felvétel megismerésére az állományilletékes parancsnok és az általa erre munkakörükénél 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.

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

135. A gépjárműben szolgálatot teljesítő állományt tájékoztatni kell arról, hogy a gépjárművön kamera került elhelyezésre.

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

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

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

139. A területi adatvédelmi tisztviselő bármikor jogosult betekinteni a kamera felvételeibe ellenőrzés céljából.

140. Az FKI vagyonszámla célú szolgáló mozgó kamerái kizárólag magánterületen, illetve a magánterületnek a közönség számára nyilvános részén használhatók.

29. Hatósági tevékenységgel kapcsolatos adatkezelési szabályok

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

142. 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.

143. A kiskorú, cselekvőképtelen vagy cselekvőképességében részlegesen korlátozott nagykorú ügyfél, tanú, szemletárgybirtokos vagy megfigyelt személy érdekében a hatóság a kiskorú, a cselekvőképtelen és a cselekvőképességében részlegesen korlátozott nagykorú ügyfél, tanú, szemletárgybirtokos vagy megfigyelt személy védelme érdekében erre irányuló kérelem nélkül is dönthet az érintett személy adatainak zárt kezeléséről és az iratbetekintési jog korlátozásáról.

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

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

146. Ügyféli minőség hiánya esetén iratbetekintést kérő személy személyes adatot tartalmazó iratba kizárólag akkor tekinthet be, ha konkrét jogérvényesítési célt, vagy megfelelő jogalapot tud igazolni, ellenkező esetben a kérelmet el kell utasítani.

147. 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.

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

30. Beavatkozásokkal kapcsolatos adatkezelési szabályok

149. 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 őrsőkön elzárva kell tárolni.

31. Szerződésekkel kapcsolatos személyes adatkezelések

150. Az FKI-val szerződéses kapcsolatban álló szervezetekkel, személyekkel kötött szerződésekben szereplő személyes adatok kezelése során az FKI által a másik szerződő fél részére továbbított személyes adatok esetében a harmadik személy jogos érdekének érvényesítése előnyt élvez a munkavállaló személyes adataihoz fűződő rendelkezési jogához képest, mivel a munkavállaló munkakörének ellátásához szükséges és arányos korlátozás.

151. Az FKI-val szerződéses kapcsolatban álló szervezetekkel, személyekkel kötött szerződésekben az alábbiakat kell feltüntetni: „A Felek képviselőinek, a Szerződés teljesítésében közreműködő személyek és a kapcsolattartók adatait a Felek a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/466EK irányelv hatályon kívül helyezéséről szóló, 2016. április 27-i (Eu) 2016/679 európai parlamenti és tanácsi rendelet (a továbbiakban: GDPR) rendelkezései szerint kezelik. A Felek a saját alkalmazottaik adatait a GDPR 6. cikk (1) bekezdés (b) pontja és a munkavégzésre irányuló jogviszonyt szabályozó jogszabály rendelkezése alapján, a Felek által a másik Fél részére továbbított személyes adatokat a GDPR 6. cikk (1) bekezdés (f) pontja szerint, a szerződéses partnerük jogos érdekében veszik át és kezelik a célhoz szükséges mértékben és ideig.”

V. Fejezet

Adatbiztonsági előírások

32. Adatbiztonsági fokozatok

152. Az adatbiztonsági intézkedések meghatározása érdekében az FKI kezelésében lévő minden egyes személyes adatot tartalmazó adatállományt az adatállományt kezelő szervezeti elem vezetőjének a védelmi igény szempontjából értékelni kell, majd a 153. pontban meghatározott biztonsági fokozatba kell sorolni. A besorolásban a területi adatvédelmi tisztviselő szükség esetén segítséget nyújt.

153. A hivatásos katasztrófavédelmi szervek adatkezelésének biztonsági fokozatai:

- a) lap adatbiztonsági fokozat: alapesetben azon adatkezelések tartoznak ebbe a fokozatba, amelyekben feldolgozott adatok közérdekből nyilvános adatok.
- b) fokozott adatbiztonsági fokozat: alapesetben azon adatkezelések tartoznak ebbe a fokozatba, amelyekben személyes adatok találhatóak.
- c) kiemelt adatbiztonsági fokozat: alapesetben ebbe a fokozatba tartoznak a különleges adatot tartalmazó adatkezelések.

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

155. Az egyes adatkezelések biztonsági fokozatának megállapításához az adatok minősítésének figyelembevételén kívül figyelembe kell venni, hogy:

- a) az adatok illetéktelen személy által történő megismerése, megváltoztatása, vagy törlése milyen mértékben veszélyezteti az adatkezelő vagy más szerv feladatainak végrehajtását,
- b) az érintett személyiségi jogainak érvényesülését,
- c) a megsérült, vagy megsemmisült adatok helyreállítása mekkora ráfordítással végezhető el,
- d) a Szabályzat 6. számú függelékében meghatározott, adatbiztonságot veszélyeztető kockázati elemek milyen mértékben érvényesülnek az adott adatállomány vonatkozásában.

156. A 155. pontban meghatározott tényezők figyelembevételével a 153. pontban meghatározottnál magasabb adatbiztonsági fokozat is meghatározható.

157. Az alap adatbiztonsági fokozatba sorolt adatállományok tekintetében figyelemmel kell lenni arra, hogy az abban található adatok naprakészek és pontosak legyenek.

158. A fokozott biztonsági fokozatba sorolt adatállományok tekintetében biztosítani kell a 157. pontban foglaltakat, továbbá, hogy azokhoz kizárólag az adatállománnyal kapcsolatos feladatot ellátó és helyettesítésére kötelezett állománytag vagy állománytagok, továbbá a munkájuk ellenőrzésére jogosult vezetők férjenek hozzá.

159. A kiemelt biztonsági fokozatba tartozó nyilvántartások tekintetében biztosítani kell a 158. pontban foglaltakat, hogy azokhoz kizárólag az adatállománnyal kapcsolatos feladatot ellátó és helyettesítésére kötelezett állománytag vagy állománytagok, továbbá a munkájuk ellenőrzésére jogosult vezetők férjenek hozzá, a hozzáféréshez az arra jogosultakat jelszóval kell ellátni.

33. Adatbiztonsági intézkedések

160. Az adatbiztonsági intézkedéseket - a vonatkozó jogszabályok és a Szabályzat keretei között – az FKI-nál a biztonságos adatkezeléshez szükséges legmagasabb biztonsági fokozatokhoz és a helyi adottságokhoz igazodva kell meghatározni és végrehajtani.

161. Az infrastruktúrához, az FKI 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.

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

34. Az adatkezelés dokumentációjának védelmére vonatkozó adatbiztonsági intézkedések

163. 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. A fokozott és kiemelt biztonsági fokozatba sorolt adatkezelések dokumentációit páncélszekrényben, vagy biztonsági zárral és falakattal

ellátott lemezszekrényben, vagy biztonsági zárral, vasráccsal és falakattal, illetve elektronikus védelemmel ellátott helyiségben kell őrizni.

164. Szabályozni kell a katasztrófavédelmi objektumokba történő be- és kilépés rendjét, beleértve a számítógépek és adathordozók ellenőrzött és dokumentált szállítását. Az informatikai eszközök elhelyezésére szolgáló épületeket, helyiségeket úgy kell kialakítani, hogy megfelelő biztonságot nyújtsanak az erőszakos behatolás, tűz vagy természeti csapás ellen (különösen megfelelő teljesítményű elektromos hálózat kialakítása, épület ellátása villámhárítóval, megelőző intézkedések a vízbetörés ellen). A lokális számítógépes hálózat központi részét tartalmazó helyiséget tervszerűen, biztonsági szempontok alapján kell kiválasztani, lehetőség szerint az épület közterülettől távolabb eső részében.

165. Megelőző intézkedésként gondoskodni kell a nyílászárók védelméről (például: rács, áttörést nehezítő üvegezés, speciális zár).

166. A számítógépes vagy az adathordozók tárolására szolgáló helyiségeket tűzvédelmi és indokolt esetben vagyonvédelmi eszközökkel el kell látni.

167. A hivatásos katasztrófavédelmi szervek helyiségeiben, különös tekintettel azokra, ahol külső személyek is jogszerűen tartózkodhatnak, kerülni kell az adatkezelések helyére, módjára történő utalást, jelzést. A számítógépet úgy kell elhelyezni, hogy a képernyőn megjelenített adatok a helyiségbe belépő, illetve a helyiségben tartózkodó személyek elől védve legyen. A bejelentkezésnél, a jelszó begépelésénél kerülni kell az illetéktelen személyek jelenlétét.

168. Hatósági ügyekben, elektronikus kapcsolattartás esetén kapcsolattartási útként kizárólag az ügyintéző, vagy a szervezeti egység hivatalos elektronikus levélcíme használható.

169. A személyi állomány tagja hivatásos katasztrófavédelmi szerv objektumában nem a hivatásos katasztrófavédelmi szerv tulajdonát képező hardvereszközt csak előjárójának vagy vezetőjének engedélyével és informatikai szakember által végzett ellenőrzést követően használhat.

170. A hivatásos katasztrófavédelmi szerv számítástechnikai eszközei csak hivatásos katasztrófavédelmi szerv objektumán belül használhatók, kivéve a külön engedély alapján használt hordozható eszközöket (laptop, winchesterek stb).

171. A fokozott és kiemelt biztonsági fokozatba tartozó adatállományok kezeléséhez igénybe vett informatikai eszközök üzemszerű működését szünetmentes áramforrásokkal áramkimaradás idejére is biztosítani kell, illetve a kiemelt biztonsági fokozatba tartozó adatok védelme érdekében sugárzásvédelmi eszközöket és módszereket kell alkalmazni.

172. Az egyedi adatkezelést végző állomány épületen belüli mozgását az anyagi-technikai lehetőségek függvényében fizikai azonosítási eszközökkel (például: speciális kulcsok, chip-kártyák) is követhetővé kell tenni.

35. A hardvereszközök védelmét szolgáló adatbiztonsági intézkedések

173. Az informatikai eszközök objektumon belüli telepítését, illetve annak irányítását az adatkezelő hivatásos katasztrófavédelmi szerv vezetője által megbízott, rendszergazdai jogosultsággal rendelkező személy végzi, akinek szakmai véleményét ki kell kérni az eszközök beszerzésének előkészítése során is.

174. Az eszközök elhelyezését, a számítógépes munkahelyek kialakítását a biztonsági szempontokra is figyelemmel kell tervezni.

175. Nem kereskedelmi forgalomban beszerzett (például: alapítványi támogatásból származó, adományozott) hardvereszközök csak előzetes ellenőrzést és engedélyezést követően vehetőek alkalmazásba és kapcsolhatók a lokális hálózatba.

176. Külső személy - például karbantartás, javítás, fejlesztés céljából - a hardvereszközökhöz kizárólag úgy férhet hozzá, hogy a kezelt adat megismerése elkerülhető legyen. A fokozott és kiemelt biztonsági fokozatba sorolt adatállományok kezeléséhez igénybe vett hardvereszközök javítása, karbantartása csak állandó felügyelet mellett végezhető.

177. A készülékekről, azok műszaki állapotváltozásairól folyamatos nyilvántartást kell vezetni (törzslap).

178. Gondoskodni kell arról, hogy a hardvereszközök, illetve azok szolgáltatásainak igénybevétele csak a felhasználó azonosítását követően legyen lehetséges.

179. Gondoskodni kell a személyes adatot tartalmazó adathordozók tárolásához szükséges környezeti feltételek (hőmérséklet, páratartalom, stb.) megteremtéséről.

180. Szabályozni kell a személyes adatokat tartalmazó adathordozókkal kapcsolatos adminisztrációs folyamatot, a felhasználás, a nyilvántartás, az átadás-átvétel rendjét.

181. A hivatásos katasztrófavédelmi szerv által működtetett számítástechnikai rendszerekben csak vírusmentesség szempontjából ellenőrzött adathordozók alkalmazhatók.

182. A felhasználók részére az adathordozók rongálás elleni védelmét szolgáló előírásokat kell meghatározni a külső jelölés módjára, a jogosulatlan hozzáférés, másolás, törlés megelőzésére. Az érintett személyi állományt e szabályok megfelelő ismerete érdekében oktatni kell.

183. A fokozott és a kiemelt biztonsági fokozatba tartozó adatállományokat tartalmazó adathordozókról biztonsági másolatot kell készíteni és azokat lehetőleg az adatállomány őrzési helyétől eltérő tűzszakaszban kell őrizni.

184. Az adatkezelő szervek személyes adatokat tartalmazó meghibásodott winchestere - az azon rögzített adatok védelme, különösen a korábban rögzített adatok helyreállításának kizárása érdekében - külső szervnek, személynek javítás vagy csere érdekében nem adható át, azt meg kell semmisíteni.

36. Az adatkezelés dokumentációjának védelmére vonatkozó adatbiztonsági intézkedések

185. 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.

186. A fokozott és kiemelt biztonsági fokozatba sorolt adatkezelések dokumentációit páncélszekrényben, vagy biztonsági zárral és falakattal ellátott lemezszekrényben, vagy biztonsági zárral, vasráccsal és falakattal, illetve elektronikus védelemmel ellátott helyiségben kell őrizni.

37. A személyhez fűződő és az alkalmazói tevékenységgel összefüggő intézkedések

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

188. 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 ügýtípus ügyirata.

VI. Fejezet

Információszabadság az FKI-nál

38. Az információszabadság tartalma

189. Az FKI-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.

190. 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.

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

39. Szerződésekkel, támogatásokkal, projektekkel kapcsolatos adatnyilvánosság és az üzleti titok

192. Az FKI-val 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, ill. közérdekből nyilvános adatnak minősülő tartalmára vonatkozóan tájékoztatást adni.”

193. Az FKI 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) és a c) pont ca) és a cd) alpontban foglalt adatok személyes adatnak minősülnek, amelyek tekintetében az adatkezelés kötelező.”

194. 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.”

40. A közérdekű adatok megismerésére irányuló igény intézésének eljárási szabályai és a költségtérítés

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

196. A közérdekű adat megismerésére irányuló igényt - a szolgálati út betartásával - soron kívül be kell mutatni az adatot kezelő szerv vezetőjének, aki a területi adatvédelmi tisztviselő útján köteles gondoskodni a megkeresés határidőben történő megválaszolásáról.

197. A BM OKF információszabadsággal foglalkozó tisztviselője intézi a BM OKF által kezelt adatokra, továbbá a BM OKF és más hivatásos katasztrófavédelmi szerv által közösen kezelt adatokra irányuló közérdekűadat-megismerési igényeket, továbbá az olyan, gazdasági adatokra irányuló kérelmeket, amelyek a BM OKF és a BM OKF GEK adatkezeléséhez egyaránt kapcsolódnak.

198. A területi adatvédelmi tisztviselő intézi az FKI 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.

199. Az FKI területi adatvédelmi tisztviselője a kérelem beérkezéséről - az adatigénylő személyes adatainak felismerhetetlenné tételével - a BM OKF információszabadsággal foglalkozó tisztviselőjét haladéktalanul értesíti. A BM OKF információszabadsággal foglalkozó tisztviselője koordinálja a hivatásos katasztrófavédelmi szervek közérdekű adatok megismerésére irányuló kérelmek teljesítésével kapcsolatos tevékenységét. A koordináció lezárultát követően a BM OKF információszabadsággal foglalkozó tisztviselője megküldi a jóváhagyott választ az FKI területi adatvédelmi tisztviselője részére, aki gondoskodik annak megküldéséről az adatigénylő részére.

200. A BM OKF információszabadsággal foglalkozó tisztviselője és az FKI területi adatvédelmi tisztviselője 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.

201. 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 - BM OKF információszabadsággal foglalkozó tisztviselője, illetve az FKI területi adatvédelmi tisztviselője haladéktalanul, de legkésőbb az igény kézhezvételét követő 5 napon belül felhívja az igénylőt az igény pontosítására.

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

203. 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.

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

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

206. 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 az FKI 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 az FKI területi adatvédelmi tisztviselője az igény kézhezvételétől számított 15 napon belül tájékoztatja a határidő meghosszabbításának okáról és a válasz várható időpontjáról.

207. Ha az igénylő az adatokat tartalmazó dokumentumról vagy dokumentumrészről másolatot kíván kérni, valamint ha az adatigény teljesítése az FKI alaptevékenységének ellátásához szükséges munkaerőforrás aránytalan mértékű igénybevételével jár, az FKI költséget állapíthat meg.

208. 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.

209. Nem állapítható meg költség az FKI azon állománytagjai tekintetében, akiknek az adatigények érdemi és adminisztratív ügyintézése munkaköri kötelezettsége, így különösen az FKI területi adatvédelmi tisztviselője, az adatok kiadhatóságára vonatkozó döntéshozatal tekintetében az FKI igazgatója, az adatigénnyel kapcsolatos érkeztetési, iktatási, kézbesítési feladatokat elvégző személy vonatkozásában, továbbá az FKI állományába nem tartozó személyek tekintetében.

210. A dologi és személyi költségek számítási módját az FKI-hoz érkezett közérdekűadat-megismerési igények teljesítésével kapcsolatos költségtérítés összegének meghatározása során alkalmazandó önköltségszámítási szabályokról szóló BM OKF főigazgatói intézkedés tartalmazza.

211. Az adatigény teljesítésénél elszámolható költségek megállapítására minden esetben sor kerül az adatokat kezelő szervezeti elemnél a *7. számú függelékben* feltüntetett dokumentum kitöltésével, számlázásra azonban csak akkor kerül sor, ha ez indokolt és a teljesítéshez szükséges munkaerő-ráfordítás időtartama meghaladja a 4 munkaórát, vagy a dologi költségek vonatkozásában a másolt oldalak száma meghaladja a 10 oldalt. A személyi és dologi költségekről az FKI Költségvetési Osztály állít ki számveteli bizonylatot.

212. A személyi és dologi költségek megállapítására van lehetőség a közérdekű adatok megismerésére vonatkozó adatigény teljesítésekor.

213. A BM OKF információszabadsággal foglalkozó tisztviselője, illetve az FKI területi adatvédelmi tisztviselője az adatigény megválaszolásában érintett szervezeti elemnek megküldi a 211. pontban meghatározott dokumentumot az adatigénnyel együtt.

214. Az érintett szervezeti elem vezetője a közérdekű adatigényben foglaltak alapján előzetesen felméri a kezelésében lévő adatok kiadására fordított munkaórát, amelyet kerekítve, az egyes munkafolyamatot végző állománytag nevének, beosztásának feltüntetésével a 211. pontban meghatározott dokumentumban rögzít.

215. Ha a személyi költségek a 4 munkaórát vagy a dologi költségek vonatkozásában a másolandó oldalak száma a 10 oldalt meghaladja, e-mailben az igényelt közérdekű adatot kezelő szervezeti elem vezetője megküldi a 223. pontban meghatározott dokumentumot a BM OKF tekintetében a Költségvetési Főosztály, területi szervek vonatkozásában a Költségvetési Osztály vezetőjének a költségszámítás elkészítése céljából.

216. Az FKI Költségvetési Osztály a rendelkezésre álló tényleges személyügyi béradatok és dologi költségek feltüntetése után, a 211. pontban meghatározott dokumentumot megküldi a BM OKF információszabadsággal foglalkozó tisztviselője, illetve területi adatvédelmi tisztviselő részére a költségek összegszerű kimutatásával.

217. A BM OKF információszabadsággal foglalkozó tisztviselője, illetve az FKI területi adatvédelmi tisztviselője a várható személyügyi és dologi kiadások összegéről a közérdekű adat megismerésére vonatkozó igény beérkezésétől számított 15 napon belül tájékoztatást küld az adatigénylő részére.

218. Ha az adatigénylés teljesítése az FKI alaptevékenységének ellátásához szükséges munkaerőforrás aránytalan mértékű igénybevételével jár, vagy 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.

219. 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 FKI által írásban meghatározott folyószámlaszámra.

220. A BM OKF információszabadsággal foglalkozó tisztviselője, illetve az FKI területi adatvédelmi tisztviselője a számveteli bizonylat elkészítése céljából az adatigénylőnek - a költségekről szóló tájékoztatóval egy időben - megküldi a *8. számú függelékben* meghatározott dokumentumot, amelyen az adatigénylő nevét és címét szükséges feltüntetni a számveteli bizonylat kiállítása céljából.

221. Az igény teljesítése során kiemelt figyelmet kell fordítani arra, hogy a közérdekű adatok közzéne ne járjon mások jogainak, vagy törvény alapján korlátozottan megismerhető adatok bizalmosságának sérelmével. Különös figyelmet kell fordítani arra, hogy az adatszolgáltatással ne kerüljenek nyilvánosságra személyes adatok, minősített adatok, törvény által nyilvánosságban korlátozott, vagy - ha az adatkezelő szerv vezetője másként nem döntött - döntéselőkészítő, nem nyilvános adatok.

222. 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.

223. Az elutasított kérelmekről, valamint az elutasítások indokairól az FKI területi adatvédelmi tisztviselője nyilvántartást vezet, és az abban foglaltakról a tárgyévet követő év január 31-éig tájékoztatja a NAIH-ot.

224. A közérdekű vagy közérdekből nyilvános adat kiadására irányuló sajtó- és médiamegkeresések intézésébe az FKI szóvivője a BM OKF információszabadsággal foglalkozó tisztviselőjét, illetve a területi adatvédelmi tisztviselőt bevonja.

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

41. A hatósági ügyekkel kapcsolatban érkező adatigények megválaszolására vonatkozó szabályok

226. Ha az adatigény hatósági ügyet érint, a megválaszolásakor az Ákr. iratbetekintési rendelkezéseiben foglalt korlátozásokat is figyelembe kell venni. Erre a válasziratban fel kell hívni az adatigénylő figyelmét.

227. Ha az igény olyan hatósági eljárás kapcsán érkezik, ami még folyamatban van, az Infotv. 27. § (5) bekezdés döntéselőkészítő 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 FKI-hoz.

228. A hatósági ügyekre vonatkozó adatigények esetén kizárólag az Ákr 33. § (5) bekezdése alapján bárki számára megismerhető határozatok adhatóak ki az anonimizálási szabályok betartásával, egyébként bármely más irat tekintetében fel kell hívni az adatigénylőt Ákr. szerinti iratbetekintési jog gyakorlására.

229. 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 iratbetekintési jog gyakorlására.

230. Ha az adatigény más hatóságok által lefolytatott eljárásokban keletkezett adatokra vonatkozik, arra az igény áttételére vonatkozó szabályokat kell alkalmazni, ideértve azt az esetet is, ha az ügyben egy másik hivatásos katasztrófavédelmi szerv járt el. Amennyiben az adatkezelőnek tudomása van arról, hogy az igényt a hatáskörrel és illetékességgel rendelkező szervhez is benyújtották, az áttétel mellőzhető.

231. Amennyiben az adatigény kizárólag szakhatósági állásfoglalás megismerésére irányul, azt az Ákr. 34. § (1) bekezdése alapján az igénylő részére önálló iratként nem lehet kiadni, hanem át kell tenni a határozatot hozó hatósághoz.

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

42. A közérdekű adatok elektronikus úton történő közzététele

233. Az elektronikus információszabadság megvalósítása érdekében a hivatásos katasztrófavédelmi szervek honlapjukon közzétételi listákat működtetnek.

234. A listák tartalmának honlapon történő elhelyezéséről a honlap szerkesztéséért felelős személy, a szóvivő vagy helyettese gondoskodik.

235. 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.

236. Az általános közzétételi listában az FKI 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.

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

238. 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.

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

240. A közzétételi lista által előírt megőrzési kötelezettség lejártakor az FKI területi adatvédelmi tisztviselője a közzétett, külön jogszabályban meghatározott közzétételi egységeket átadja a központi elektronikus jegyzék működtetője részére.

241. A közzétételi listában nem szereplő közérdekű adatokra vonatkozó adatigénylések adatai alapján az FKI területi adatvédelmi tisztviselője legalább évente felülvizsgálja az Igazgatóság egyedi közzétételi listáját, és a jelentős arányban vagy mennyiségben felmerült adatigénylések alapján azt kiegészíti.

242. A 9. számú függelék tartalmazza az FKI közzétételi listáit és a listák egyes részei tekintetében adatszolgáltatásra kötelezett szervezeti elemek megjelölését. Az adatfelelős személyt az adatfelelős szervezeti elem vezetője jelöli ki.

243. Az adatfelelős személyek a közzétételi listákban meghatározott adatokat közvetlenül vagy az adatfelelős szervezeti elem útján, elektronikus úton küldik meg az FKI területi adatvédelmi tisztviselőjének, aki az adatokat továbbítja a szóvivőnek mint adatközlőnek, amely gondoskodik a továbbított közérdekű adatok honlapon történő nyilvánosságra hozataláról.

244. Az adatfelelős személyek gondoskodnak a közreműködésükkel közzétett adatok naprakészségének figyelemmel kíséréséről, és szükséges esetben a közzétételi listán adott adatfajta 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.

245. A közzétételi listákba feltöltött adatok helytállóságáért az adatfelelős személy, a kapott adatok feltöltéséért az adatközlő, a listák egyes részei feltöltöttségének ellenőrzéséért az FKI területi adatvédelmi tisztviselője felel.

246. A helyi és szakmai szervezeti elemek - mint adatfelelősök - a tevékenységükre vonatkozó közérdekű adatokat a felettes, központi szervezeti elemnek küldik meg, ami gondoskodik a megküldött közérdekű adatok közzétételéről a szóvivő útján.

247. Az adatfelelős, valamint a honlapon adatközlést intéző személyek feladatait munkaköri leírásukban rögzíteni kell.

248. Az Egységes Közadatkereső Rendszerben és a Központi Jegyzékben történő közzétételt az FKI területi adatvédelmi tisztviselője folyamatosan végzi.

VII. Fejezet

Ellenőrzés

249. Az adatkezelési rendelkezések betartásának ellenőrzésére jogosult:

- a) az FKI igazgatója vagy az általa írásban kijelölt személy;
- b) az FKI 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 FKI Ellenőrzési Szolgálatának állományának erre írásban felhatalmazott tagja;
- e) a belügyminiszter által írásban felhatalmazott személy;
- f) a jogszabályban erre felhatalmazott személy.

250. 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 betekinhet, amely az ellenőrzött szerv adatkezelési tevékenységével összefügg.

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

252. Az FKI adatvédelmi tevékenységének céllenőrzését a BM OKF adatvédelmi tisztviselője vagy az FKI szakirányítására jogosult szerv vezetője rendelheti el.

253. A naplózási kötelezettség teljesítését a naplót vezető közvetlen szolgálati elöljárója legalább háromhavonta ellenőrizni köteles.

254. A területi adatvédelmi tisztviselő által végzett ellenőrzés elsősorban az alábbiakra terjed ki:

- a) közzétételi listák állapota;
- b) személyes adatok kezelése az ellenőrzött szerv szervezeti elemeinél;
- c) adatkezelői nyilvántartás állapota;
- d) az ellenőrzött szervezeti elem által vezetett nyilvántartások adatvédelmi megfelelősége;
- e) a Humán Szabályzatban foglalt adatvédelmi rendelkezések megtartása;
- f) az adatbiztonság követelményeinek való megfelelés.

255. A területi adatvédelmi tisztviselő legalább negyedévente köteles ellenőrizni a szerv közzétételi listáinak feltöltöttségét.

256. A területi adatvédelmi tisztviselő minden félévben köteles ellenőrizni 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.

257. A területi adatvédelmi tisztviselő – a helyi adatvédelmi tisztviselők bevonásával – legalább két évente köteles ellenőrizni a szakterületek adatkezelési tevékenységét és a dolgozói adatkezeléseket.

258. Az ellenőrzés során feltárt hiányosságokról, esetleges jogszabály- vagy normasértésekről az ellenőrzést végző az ellenőrzés befejezését követően írásban köteles tájékoztatni az FKI igazgatóját, 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

Oktatás, vizsgáztatás, tájékoztatás

259. Az FKI állományába újonnan került olyan személyeket, akik munkakörüknél fogva személyes adatokat kezelnek, a helyi adatvédelmi tisztviselők a kirendeltségek és az irányításuk alá tartozó szervezeti elemek, míg a területi adatvédelmi tisztviselő a központi szervezeti elemek vonatkozásában kötelesek az állományba vételt követő 3 hónapon belül - az FKI személyzeti feladatot ellátó szervezeti elemével történő rendszeres egyeztetés alapján - adatvédelmi oktatásban részesíteni és részükre a szükséges jogszabályokat, belső normákat és egyéb segédanyagokat rendelkezésre bocsátani, majd az oktatást követő három hónapon belül vizsgáztatásukat elvégezni.

260. Az oktatásról és a vizsgáról szóló igazolást az adatvédelmi tisztviselő a fizikai adatbiztonság szabályainak megfelelően kezeli.

261. A 259. pontban vázolt munkamegosztásban a helyi és a területi adatvédelmi tisztviselők az FKI 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. Ilyennek minősül jelen Szabályzat hatályba lépése is, melyet követően továbbképzést tartanak az adatvédelmi tisztviselők.

1. számú függelék a 10/2020. számú FKI igazgatói intézkedéshez

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

18. Hogyan biztosítja az érintettek jogainak érvényesítését?

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

20. Milyen módszerekkel kívánja csökkenteni az azonosított kockázati tényezőket?

21. Hogyan ellenőrzi az adatok teljességét?

22. Megfelelően naprakészek-e a gyűjtött adatok? Ha igen, támassa alá válaszát!

23. Kifejtett és részletezett az adatok természete?

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

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

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

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

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

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

2. számú függelék a 10/2020. számú FKI igazgatói intézkedéshez

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:

- adatkezelés jellege, hatóköre, körülményei;
- a személyes adatok, a címzettek, valamint a személyes adatok tárolási időtartamának meghatározása;
- funkcionális leírás az adatkezelési műveletről;
- módszeres leírás az adatfeldolgozásról, az adatkezelés céljainak ismertetésére, beleértve adott esetben az adatkezelő által érvényesíteni kívánt jogos érdeket;
- jogalap meghatározása;
- a személyes adatokhoz használt eszközök (hardverek, szoftverek, hálózatok, személyek, papírok vagy papíralapú továbbítási csatornák) megnevezése;
- 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;
- az adatkezelésre vonatkozó, rendelkezésre álló igazgatási rendszerterv, vagy folyamatleírás bemutatása;
- hatásvizgálatra vonatkozó szerep- és felelősségi körök meghatározása.

2. Az adatkezelési műveletek szükségességi és arányossági vizsgálata:

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

- 1) a lehetséges kockázati tényezők azonosítása,

2) a kockázati tényezők értékelése,

3) a kockázati tényezők csökkentésére, megszüntetésére irányuló javaslatok megfogalmazása.

A kockázati tényezők azonosításában nagy szerepe van továbbá az érintettekkel való konzultációnak. A 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 lehetőségekre. 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 adataitanyai 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. számú 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 9. cikkben meghatározott különleges kategóriái (például az egyének politikai véleményére vonatkozó adatok), valamint a 10. cikkben 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 általános adatvédelmi 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: az általános adatvédelmi rendelet nem határozza meg, mi értendő nagy szám alatt, jóllehet a (91) preambulum bekezdés nyújt némi iránymutatást. Mindenesetre a 29. cikk 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 (75. preambulum bekezdés): 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 jogukat 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 általános adatvédelmi rendelet egyértelműen megfogalmazza [a 35. cikk (1) bekezdése, valamint a (89) és a (91) preambulum bekezdés], hogy „a technológia elismert állásának megfelelő” módon meghatározott új technológia [(91) preambulum bekezdés] használata szükségessé teheti az adatvédelmi hatásvizsgálat elvégzését. 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 jogukat gyakorolják vagy szolgáltatásokat vegyenek igénybe vagy szerződést érvényesítsenek”[22. cikk és (91) preambulum bekezdés]. 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” [a 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 [a 35. cikk (1) bekezdése];

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

- ha a 6. cikk (1) bekezdésének 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 [a 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. számú függelék a 10/2020. számú FKI igazgatói intézkedéshez**Minta**(adatvédelmi tájékoztató és hozzájáruló nyilatkozat kép- vagy kép- és hangfelvételen történő szerepléshez állománytagok részére)*

TÁJÉKOZTATÓ SZEMÉLYES ADAT KEZELÉSÉRŐL

A kép- vagy kép- és hangfelvételeken (a továbbiakban: felvétel) történő részvétel kapcsán /pl. a jutalom, elismerés átvételének képi dokumentálása, folyóiratban készült interjúhoz készült képfelvétel, a beavatkozáshoz, munkavégzéshez kapcsolódó, de nem a tevékenységről készített portrészzerű felvételek/ a képmás - mint személyes adat - kezelésére a Polgári Törvénykönyvről szóló 2013. évi V. törvény 2:48. § (1) bekezdése alapján, és az Európai Parlament és a Tanács (EU) 2016/679 rendelete 6. cikk (1) bekezdés a) pontja alapján az érintett hozzájárulásával kerül sor.

Kivételt képez a teljes személyi állomány tekintetében, hogy a tömegfelvételeken történő szerepléshez (pl. állománygyűlésen készített, nem portrészzerű képek) vagy a nyilvános közéleti szereplés során készített képek készítéséhez nem szükséges az érintettek hozzájárulása.

A beavatkozó - vagy egyébként közterületen a katasztrófavédelem hatáskörében eljárva munkát végző - állományról a beavatkozás, szolgálatteljesítés ideje alatt, a katasztrófavédelmi tevékenységhez kapcsolódó időszerű, napi eseményekről történő tájékoztatás céljából kép- vagy kép- és hangfelvételek készítéséhez szintén nem szükséges az érintettek hozzájárulása.

A kivételi körök meghatározására a Ptk. 2:48. § (2) bekezdése alapján, továbbá a Fővárosi Törvényszék 56.Pf.632.194/2015/3. számú ítélete alaptörvény-ellenességének megállapításáról és megsemmisítéséről szóló 16/2016. (X. 20.) AB határozat és a Kúria Pfv.IV.20.283/2015/4. számú ítélete, valamint a Fővárosi Ítéltábla 2.Pf.20.186/2014/4. számú ítélete alaptörvény-ellenességének megállapításáról és megsemmisítéséről szóló 17/2016. (X. 20.) AB határozatban foglaltakra tekintettel került sor.

1. Az adatkezelés célja a közvélemény tájékoztatása a katasztrófavédelmi tevékenység körébe tartozó időszerű, napi eseményekről, vezetők tekintetében a katasztrófavédelem vezetőit bemutató oldalon történő megjelenítés.

2. A kezelt személyes adat a képmás, és a felvétel készítésének időpontjában az érintett által tanúsított viselkedés, a megnyilvánuló érzelmi állapot.

3. A képfelvétel kapcsán adatkezelő a BM Országos Katasztrófavédelmi Főigazgatóság/Fővárosi Katasztrófavédelmi Igazgatóság/Katasztrófavédelem című folyóirat szerkesztősége [a megfelelő adatkezelő(k) kiválasztandó(ak) több adatkezelő esetén mindegyiket meg kell nevezni, és a 4. pontban mindegyik adatkezelő adatait meg kell adni]

4. Az adatkezelő adatai:

Az adatkezelő megnevezése:

Székhelye:

Postai címe:

Telefonszáma:

Telefaxszáma:

Elektronikus levélcíme:

Adatvédelmi tisztviselő: Szolgálati helye:

Elérhetősége (elektronikus levélcím, telefonszám):

5. A képfelvételek a hivatásos katasztrófavédelmi szervek honlapján, a Katasztrófavédelem Médiaszerverén, a Katasztrófavédelem hivatalos Facebook oldalán tehetőek közzé, az ott meghatározott Adatvédelmi Irányelveknek megfelelően, továbbá megjelenhetnek a Katasztrófavédelem című elektronikus folyóiratban is. A Médiaszerverre feltöltött kép- és hangfelvételeket a sajtó és média képviselői kizárólag a katasztrófavédelmi tevékenység bemutatása céljából, a Felhasználási Feltételeknek megfelelően vehetik át.

6. A honlapokon történő közzététel és a Médiaszerver szempontjából a technikai hátteret biztosító Rádiós Segélyhívó és Infokommunikációs Országos Egyesület adatfeldolgozónak minősül, egyéb esetek az adatok feldolgozását az adatkezelő saját szervezetén belül, önállóan végzi.

Az adatfeldolgozó postacíme: 1089 Budapest, Elnök utca 1.

Telefonszáma:(+36-1) 303-0168

Telefaxszáma:(+36-1) 477-0549

Elektronikus levélcíme: info@rsoe.hu

Honlapja: www.rsoe.hu

7. A felvételeket - ha az érintett később nem kéri azok törlését - az adatkezelő az archívumában selejtezés nélkül megőrzi.

8. A képfelvétel készítéséhez hozzájárulást nem adó személyek jogának biztosítása érdekében azon állománytagok nevét, akik nem kívánnak a felvételeken szerepelni, e joguk érvényesítése érdekében - nevet, rendfokozatot, beosztást, vonulós állomány esetén a szolgálati csoportot is megjelölve - az érintettet foglalkoztató hivatásos katasztrófavédelmi szerv adatvédelmi tisztviselője nyilvántartásba veszi, majd az aktualizált nyilvántartást átadja a kommunikációért felelős területen e feladatra kijelölt, kép- vagy kép- és hangfelvételeket készítő személyeknek. A nyilvántartott neveket kizárólag a felvételekkel kapcsolatos adatkezelést végző személyek, valamint az adatvédelmi tisztviselő ismerhetik meg. Amennyiben egy rendezvényen, eseményen több hivatásos katasztrófavédelmi szerv állománytagjai vesznek részt, és a résztvevő állománytagok nyilatkozata kiterjedt a rendezvényt szervező hivatásos katasztrófavédelmi szerve, az érintettet foglalkoztató hivatásos katasztrófavédelmi szerv szóvivője tájékoztatást nyújt a rendezvényt szervező hivatásos katasztrófavédelmi szerv szóvivője, központi rendezvény esetén a BM OKF Kommunikációs Szolgálat részére a hozzájárulás hiányát illetően. Az adatvédelmi tisztviselő az érintettet az adatkezelő állományából történő kikerülésekor törli a nyilvántartásból.

9. Az adatkezelő a személyes adatokat védi 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.

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 25 napon belül, a megadott elérhetőségre küldött levélben teljesíti.

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 25 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 25 napon belül teljesíti, és erről a megadott elérhetőségre értesítést küld.

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. § 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 Könyvének Harmadik Része, valamint a polgári perrendtartásról szóló 2016. évi CXXX. törvény 502.-503. §-ai alapján bírósághoz fordulhat.

A Nemzeti Adatvédelmi és Információszabadság Hatóság elérhetősége:

Postacím: 1530 Budapest, Pf.: 5.

Telefon: +36 (1) 391-1400

Elektronikus postacím: ugyfelszolgalat@naih.hu

Honlap: www.naih.hu

HOZZÁJÁRULÓ NYILATKOZAT SZEMÉLYES ADAT KEZELÉSÉHEZ

Alulírott, (név, szolgálati hely) a fenti tájékoztatóban írottakat tudomásul veszem, és hozzájárulok ahhoz, hogy a jelen nyilatkozathoz tartozó tájékoztatóban megjelölt adatkezelő a katasztrófavédelmi tevékenység bemutatása céljából engem ábrázoló felvételt készítsen és azt a tájékoztató szerinti helyeken és feltételek mellett nyilvánosságra hozza.

Kelt.:

Érintett aláírása

HOZZÁJÁRULÓ NYILATKOZAT SZEMÉLYES ADAT KEZELÉSÉHEZ

Alulírott, (név, szolgálati hely) a fenti tájékoztatóban írottakat tudomásul veszem, és hozzájárulok ahhoz, hogy a jelen nyilatkozathoz tartozó tájékoztatóban megjelölt adatkezelő a katasztrófavédelem vezetőit bemutató oldalon történő közzététel céljából engem ábrázoló felvételt készítsen és azt a tájékoztató szerinti helyeken és feltételek mellett nyilvánosságra hozza.

Kelt.:

Érintett vezető aláírása

NYILATKOZAT SZEMÉLYES ADAT KEZELÉSÉHEZ

Alulírott, (név, szolgálati hely) a fenti tájékoztatóban írottakat és a hozzájárulásomat nem igénylő adatkezeléseket tudomásul veszem, azon túl azonban nem járulok hozzá az engem ábrázoló képfelvétel készítéséhez.

Kelt.:

Érintett aláírása

4. számú függelék a 10/2020. számú FKI igazgatói intézkedéshez

Minta

(adatvédelmi tájékoztató és hozzájáruló nyilatkozat kép- vagy kép- és hangfelvételen szerepléshez állományon kívüli személyek részére)

TÁJÉKOZTATÓ SZEMÉLYESADAT-KEZELÉSRŐL

A kép- vagy kép- és hangfelvételeken (a továbbiakban: felvétel) történő részvétel kapcsán az adatkezelésre a Polgári Törvénykönyvről szóló 2013. évi V. törvény (a továbbiakban: Ptk.) 2:48. § (1) bekezdése alapján, és az Európai Parlament és a Tanács (EU) 2016/679 rendelete 6. cikk (1) bekezdés a) pontja alapján az érintett hozzájárulásával kerül sor.

Kivételt képez a tömegfelvételeken történő szereplés megörökítése vagy a nyilvános közéleti szereplés során készített képek készítése, melyekhez nem szükséges az érintettek hozzájárulása.

1. Az adatkezelés célja a közvélemény tájékoztatása a katasztrófavédelmi tevékenység körébe tartozó időszakú, napi eseményekről, ennek keretében a rendezvényről/eseményről.

2. A kezelt személyes adat a képmás, és a felvétel készítésének időpontjában az érintett által tanúsított viselkedés, a megnyilvánuló érzelmi állapot.

3. A képfelvétel kapcsán adatkezelő a BM Országos Katasztrófavédelmi Főigazgatóság/Fővárosi Katasztrófavédelmi Igazgatóság/Katasztrófavédelem című folyóirat szerkesztősége [a megfelelő adatkezelő(k) kiválasztandó(ak) több adatkezelő esetén mindegyiket meg kell nevezni, és a 4. pontban mindegyik adatkezelő adatait meg kell adni]

4. Az adatkezelő adatai:

Az adatkezelő megnevezése:

Székhelye:

Postai címe:

Telefonszáma:

Telefaxszáma: Elektronikus levélcíme:

Adatvédelmi tisztviselő:

Szolgálati helye:

Elérhetősége (telefon, elektronikus levélcím):

5. A képfelvételek a hivatásos katasztrófavédelmi szervek honlapján, a Katasztrófavédelem Médiaszerverén, a Katasztrófavédelem hivatalos Facebook oldalán tehetőek közzé, az ott meghatározott Adatvédelmi Irányelveknek megfelelően, továbbá megjelenhetnek a Katasztrófavédelem című elektronikus folyóiratban is. A Médiaszerverre feltöltött kép- és hangfelvételeket a sajtó és média képviselői kizárólag a katasztrófavédelmi tevékenység bemutatása céljából, a Felhasználási Feltételeknek megfelelően vehetik át.

6. A honlapokon történő közzététel és a Médiaszerver szempontjából a technikai hátteret biztosító Rádiós Segélyhívó és Infokommunikációs Országos Egyesület adatfeldolgozónak minősül, egyéb esetek az adatok feldolgozását az adatkezelő saját szervezetén belül, önállóan végzi.

Az adatfeldolgozó postacíme: 1089 Budapest, Elnök utca 1.

Telefonszáma:(+36-1) 303-0168

Telefaxszáma:(+36-1) 477-0549

Elektronikus levélcíme: info@rsoe.hu

Honlapja: www.rsoe.hu

7. A felvételeket - ha az érintett később nem kéri azok törlését - az adatkezelő az archívumában selejtezés nélkül megőrzi.

8. Az adatkezelő a személyes adatokat védi 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.

9. 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 25 napon belül, a megadott elérhetőségre küldött levélben teljesíti.

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 25 napon belül teljesíti, és erről a megadott elérhetőségre küldött levélben értesíti.

A törléshez való jog: a tájékoztatóban felsorolt elérhetőségeken kérheti az adatkezelőtől adatainak törlését. Az adatkezelő az adattörlés iránti kérelem teljesítését abban az esetben tagadhatja meg, ha azokat jogszabály alapján kötelező kezelnie. Egyéb esetben a kérelmet legfeljebb 25 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. § alapján a Nemzeti Adatvédelmi és Információszabadság Hatóságnál bejelentést tehet, továbbá az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény 23. §-a szerint, valamint a Polgári Törvénykönyvről szóló 2013. évi V. törvény Második Könyvének Harmadik Része, a polgári perrendtartásról szóló 2016. évi CXXX. törvény 502.-503. §-ai alapján bírósághoz fordulhat.

A Nemzeti Adatvédelmi és Információszabadság Hatóság elérhetősége:

Postacím: 1530 Budapest, Pf.: 5.

Telefon: +36 (1) 391-1400

Elektronikus postacím: ugyfelszolgalat@naih.hu

Honlap: www.naih.hu

HOZZÁJÁRULÓ NYILATKOZAT SZEMÉLYES ADAT KEZELÉSÉHEZ

Alulírott, a fenti tájékoztatóban írottakat tudomásul veszem, és hozzájárulok ahhoz, hogy a jelen nyilatkozathoz tartozó tájékoztatóban megjelölt adatkezelő(k) a katasztrófavédelmi tevékenység bemutatása céljából engem ábrázoló felvételt készítsen, és azt a tájékoztató szerinti helyeken és feltételek mellett nyilvánosságra hozza.

Budapest,

Érintett aláírása

5. számú függelék a 10/2020. számú FKI igazgatói intézkedéshez

Minta (adatvédelmi tájékoztató és hozzájáruló nyilatkozat projektekben történő részvételhez)

TÁJÉKOZTATÓ PROJEKTBEN TÖRTÉNŐ RÉSZVÉTEL KAPCSÁN TÖRTÉNŐ SZEMÉLYESADAT-KEZELÉSRŐL

1. A projektben történő részvétel során személyes adatok kezelésére az alábbi törvényhelyek alapján kerül sor

- a) az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) 5.§ (1) bekezdésének a) pontjában meghatározott kötelező adatkezelés esetén, vagyis ha azt törvény közérdeken alapuló célból elrendeli, jelen esetben, ha az adat közérdekből nyilvános adatnak minősül (Az Info tv. 27. § (3) bekezdés szerint közérdekből nyilvános adat az európai uniós támogatás felhasználásával kapcsolatos adat.)
- b) az Infotv. 5. § (1) bekezdésének d) pontja alapján az érintett hozzájárulásával;

2. Az adatkezelés célja: Pénzügyi és szakmai elszámolás biztosítása, ennek érdekében a projektben résztvevő személyek részvételének, a részükre történt kifizetések teljesítésének igazolása. A projekt közérdekből nyilvános adatainak biztosítása.

Projekt azonosító száma:

Projekt címe:

3. Az adatkezeléssel érintettek köre:

A (adatkezelő megnevezése) személyi állományának a projekttel kapcsolatos feladatokban részt vevő tagjai.

4. A kezelt adatok köre, besorolása:

- személyes adat (lakhely, anyja neve, születési hely, dátum, képi dokumentáció esetén fénykép)
- közérdekből nyilvános adat (név, beosztás, munkakör, illetmény, cafetéria)

5. Az adatkezelők, adatfeldolgozók megnevezése:

Az adatkezelő neve:

Székhelye:

Postai címe:

Telefonszáma:

Telefaxszáma:

Az adatkezelés tényleges helye:

Hozzáférésre jogosultak köre:

Adattovábbítás az alábbi szerv felé történik:

Ellenőrzést végző szerv:

Irányító hatóság:**Az adatkezelő által igénybe vett adatfeldolgozó:**

A projekt dokumentáció részét képező felvételeket az Adatkezelő a *BM OKF / Fővárosi Katasztrófavédelmi Igazgatóság (megfelelő kiválasztandó)* weboldalán hozza nyilvánosságra.

Az adatkezelés időtartama

A személyes adatok kezelése a társfinanszírozási támogatási kérelem előkészítésével kezdődik és az adatok törléséig tart. A törlésre akkor kerülhet sor, ha a vonatkozó uniós és nemzeti jogszabályok szerint a projekttel kapcsolatos dokumentum-megőrzési kötelezettség megszűnik.

6. Az érintett jogai

Az adatkezelés kapcsán tájékoztatáskéréshez való jog körében az adatkezelőtől tájékoztatás kérhető arról, hogy az adatkezelő a tájékoztatóban megjelölt adatokat

- 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 adatokat,
- előfordult-e személyes adatai tekintetében adatvédelmi incidens.

A helyesbítéshez való jog körében ha a kezelt személyes adatok pontatlanok, helytelenek vagy hiányosak az érintett kérheti az adatok pontosítását, helyesbítését vagy az érintett által rendelkezésre bocsátott adatokkal vagy nyilatkozattal való kiegészítést.

Az érintettnek a korlátozáshoz való joga alapján, ha az érintett vitatja az adatkezelő által kezelt személyes adatok pontosságát, helytállóságát vagy hiánytalanságát, és a kezelt személyes adatok pontossága, helytállósága vagy hiánytalansága kétséget kizáróan nem állapítható meg, a fennálló kétség tisztázásnak időtartamára, az érintett kérésére, az adatkezelő az adatkezelés korlátozásának időtartama alatt a korlátozással érintett személyes adatokkal a tároláson túl egyéb adatkezelési műveletet kizárólag az érintett jogos érdekének érvényesítése céljából vagy törvényben, nemzetközi szerződésben, illetve az Európai Unió kötelező jogi aktusában meghatározottak szerint végezhet.

A törléshez való jog az érintett azon joga, hogy kérése esetén az adatkezelő kezelésében lévő adatokat törölje. Mivel az adatkezelő kötelező adatkezelést végez, az érintett adatok törlése nem kérhető.

A fenti kérelmeket az adatkezelő legfeljebb 25 napon belül, a megadott elérhetőségre küldött értesítéssel egyidejűleg teljesíti.

A fenti kérelmeket az FKI adatvédelmi tisztviselője részére a dpo@katved.gov.hu elektronikus levélcímre, vagy az FKI postacímére kell előterjeszteni.

Adatbiztonság

Az FKI mint adatkezelő, az Infotv. 25/A. §-a alapján minden szükséges lépést megtesz, hogy biztosítsa az adatkezelés jogszerűségét, a személyes adatok biztonságát.

Jogorvoslat

Ha az érintett úgy érzi, hogy az adatkezelés során sérelem érte, annak tényét a helyzet rendezése érdekében az FKI adatvédelmi tisztviselője felé jelezheti. Az FKI adatvédelmi tisztviselője dr. Cseh Zoltán ra. (dpo@katved.gov.hu).

Amennyiben a megkeresés nem vezetett eredményre, az érintett az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény 52. § 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 Könyvének Harmadik Része, valamint a képfelvételek tekintetében a polgári perrendtartásról szóló 2016. évi CXXX. törvény 502-503. §-ai alapján bírósághoz fordulhat.

A Nemzeti Adatvédelmi és Információszabadság Hatóság elérhetősége:

Postacím: 1530 Budapest, Pf.: 5.

Telefon: +36 (1) 391-1400

Elektronikus postacím: ugyfelszolgalat@naih.hu

Honlap: www.naih.hu

*6. számú függelék a 10/2020. számú FKI igazgatói intézkedéshez***Az adatbiztonságot veszélyeztető főbb kockázati elemek**

1. A külső fenyegető tényezők:

- a) természeti katasztrófa;
- b) külső személy által elkövetett erőszakos cselekmény;
- c) közműellátási zavarok;
- d) külső személy tartózkodása a katasztrófavédelemi objektumban (ügyfelfogadás, látogatás, munkavégzés);
- e) védelmi berendezések technikai hibája, vészhelyzet (pl. rövidzárlat, tűz, csőtörés).

2. A hardver eszközök fenyegetettsége:

- a) műszaki jellegű hibák, rendellenességek;
- b) káros környezeti hatás (feszültségingadozás, szennyeződés, elektromágneses sugárzás, elektrosztatikus feltöltődés);
- c) a berendezések kezelésével, karbantartásával kapcsolatos hibák;
- d) perifériákhoz való illetéktelen hozzáférés;
- e) a berendezések manipulálása, rongálása, lopás;
- f) az eszköz elhelyezésére szolgáló helyiség, vagy munkahely helytelen kiválasztása.

3. Az adathordozók veszélyeztetettsége:

- a) gyártási hiba;
- b) károsodás nem szabályszerű tárolás, vagy kezelés miatt;
- c) ismeretlen, vagy kétes eredetű adathordozó alkalmazása;
- d) kontroll nélküli hozzáférés az adathordozókhoz, másolás;
- e) saját adathordozó ellenőrzés nélküli alkalmazása szolgálati vagy magáncélra (vírusveszély, illegális másolás).

4. Az iratokhoz, informatikai dokumentációkhoz kapcsolódó kockázati elemek:

- a) a rendszerdokumentáció teljes, vagy részleges hiánya;
- b) az iratok követhető rendszerezettségének hiánya;
- c) az aktualitás hiánya;
- d) jogosulatlan, hibás, ismeretlen eredetű változtatás;
- e) kontroll nélküli hozzáférés, sokszorosítás.

5. A szoftverekhez kapcsolódó veszélyforrások:

- a) nem jogtiszt, ismeretlen szoftver alkalmazása;

- b) szoftverhiba;
- c) jogosulatlan hozzáférés, másolás lehetősége;
- d) szoftver ellenőrizetlen bevitele az informatikai rendszerbe;
- e) vírusveszély;
- f) szándékos vagy gondatlan kezelési, karbantartási hiba;
- g) a szoftver sérülése, károsodása hardver hiba miatt;
- h) dokumentációk hiánya, sérülése.

6. Az alkalmazói tevékenységgel, adatokkal összefüggő kockázati elemek:

- a) adatvesztés, károsodás hardver vagy szoftver hiba miatt;
- b) teljes, vagy részleges adatvesztés hibás adathordozó miatt;
- c) a jogosult adatkezelő által szándékosan vagy tévedésből végzett adattörlés, -módosítás;
- d) jogosulatlan adatkezelő által végzett másolás, törlés, módosítás;
- e) hibás adatkezelés ismerethiány miatt;
- f) kezelési előírások, oktatás hiánya.

7. Fenyegető tényezők a kommunikáció területén:

- a) jogosulatlanok bejutása a hálózatba nem ellenőrizhető csatlakozás révén;
- b) hálózati hardverek és szoftverek szándékos vagy gondatlan manipulálása;
- c) adatforgalom lehallgatása;
- d) váratlan forgalmazási akadályok, az átvitelt zavaró befolyások;
- e) üzenetvesztés, üzenet megváltoztatása;
- f) az adatátviteli eszközök sérülése, károsodása.

8. Személyhez fűződő veszélyforrások:

- a) hibás adatkezelés ismerethiány vagy fáradtság, figyelmetlenség miatt;
- b) az adatkezelésre vonatkozó előírások figyelmen kívül hagyása hiányos „biztonságtudat” miatt, a fenyegetettség lebecsülése;
- c) szándékosan hibás adatkezelés belső készítés vagy külső ráhatás következményeként;
- d) jogosulatlan hozzáférés;
- e) az ellenőrzés hiánya.

7. számú függelék a 10/2020. számú FKI igazgatói intézkedéshez

KIMUTATÁS

közérdekű adat megismerésére vonatkozó igényrel kapcsolatos költség előzetes és utólagos
elszámolásához, munkaidő-elszámoláshoz

.....-...../20.../ számú ügyirathoz

1. Adatszolgáltatás előkalkulációhoz:

Az adatszolgáltatásért felelős vezető megnevezése:

Feladatvégzésre kijelölt neve:

Feladatvégzésre kijelölt beosztása:

A feladat megérkezésének időpontja:

Feladatvégzés tervezett munkaidőigénye: óra

Feladatvégzés tervezett anyagköltsége:

adatok lapban

színes fekete-fehér

Fénymásolatok száma A/4

A/3

Feladatvégzéshez szükséges adathordozók száma: db

Az adatszolgáltatásért felelős vezető aláírása:

2. Adatszolgáltatás várható költsége:

Költségvetési Főosztály/Osztály vezetőjének nyilatkozata az adatigénylés várható költségéről:

Dologi költség:

Személyi költség:

Összesen:

4 munkaórát meghaladja: igen/nem

Az összeghatár mértéke az 5000 Ft-ot meghaladja: igen/nem

Számviteli bizonylat kiállítható: igen/nem

.....aláírás/dátum

3. Munkalap:

Kezdés Befejezés

.....

Összesen: óra

Feladatvégzés anyagköltsége:

adatok lapban

színes fekete-fehér

Fénymásolatok száma A/4

A/3

Feladatvégzéshez igénybe vett adathordozók száma: db

A feladat elvégzését követően az ügyintéző aláírása:

A feladat elvégzését igazoló vezető aláírása:

4. Tényleges költségek kimutatása:

Pénzügyi/személyügyi szervezeti egység bérkimutatása (óra/Ft)

Dologi költség:

Személyi költség:

Összesen:

Pénzügyi vezető aláírása:

Minden ügyintéző külön munkaidő-elszámolást tölt ki.

A kitöltött és aláírt elszámolást a BM OKF információszabadsággal foglalkozó tisztviselője, illetve a területi adatvédelmi tisztviselő részére kell elektronikusan megküldeni.

8. számú függelék a 10/2020. számú FKI igazgatói intézkedéshez

Adatlap az Infotv. 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:

Székhelye:

Postai címe:

Telefonszáma:

Telefaxszáma:

Adatvédelmi tisztviselője:

Szolgálati helye:

Elektronikus levélcíme:

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 25 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 25 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 25 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. § 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 Könyvének Harmadik Része, a polgári perrendtartásról szóló 2016. évi CXXX. törvény 502-503. §-ai alapján bírósághoz fordulhat.

A Nemzeti Adatvédelmi és Információszabadság Hatóság elérhetősége:

Postacím: 1530 Budapest, Pf.: 5.

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

*9. számú függelék a 10/2020 számú FKI igazgatói intézkedéshez
külön xlsx állomány*



10 függelék területi listák.xlsx