

## 25/2018. (XII. 28.) BM utasítás

### **a Belügyminisztérium adatvédelmi, adatbiztonsági és közérdekű adat megismerésére vonatkozó szabályzatának kiadásáról<sup>1</sup>**

A jogalkotásról szóló 2010. évi CXXX. törvény 23. § (4) bekezdés *c*) pontjában meghatározott hatáskörömben eljárva - tekintettel az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény 25/M. § (1) bekezdés *f*) pontjában és 30. § (6) bekezdésében meghatározottakra és a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről szóló Európai Parlament és Tanács 2016/679 számú rendelet 24. cikk (2) bekezdésében vonatkozó szabályokra - a Belügyminisztérium által kezelt személyes adatok védelme érdekében a következő utasítást adom ki:

1. § A Belügyminisztérium adatvédelmi, adatbiztonsági és közérdekű adat megismerésére vonatkozó szabályzatát az 1. mellékletben foglaltak szerint határozom meg.

2. § Ez az utasítás a közzétételét követő ötödik napon lép hatályba.

3. §<sup>2</sup>

#### 1. melléklet a 25/2018. (XII. 28.) BM utasításhoz

### ***A Belügyminisztérium adatvédelmi, adatbiztonsági és közérdekű adat megismerésére vonatkozó szabályzata***

#### I. FEJEZET

#### ÁLTALÁNOS RENDELKEZÉSEK

1. Az utasítás hatálya kiterjed a Belügyminisztérium (a továbbiakban: minisztérium) szervezeti egységeire, a szervezeti egységek kezelésében lévő közérdekű adatokra és közérdekből nyilvános adatokra vonatkozó, az információs szabadsággal kapcsolatos követelmények teljesülésének biztosítására.

1.1. A minisztérium adatkezelési tevékenységében állandó vagy eseti jelleggel résztvevő vagy abban közreműködő, a minisztérium érdekkörében adatfeldolgozóként vagy közös adatkezelőként eljáró természetes és jogi személyekkel, jogi személyiséggel nem rendelkező szervezetekkel kötendő szerződésekben, megállapodásokban érvényesíteni kell a személyes adatok kezelésére vonatkozóan az utasításban meghatározott követelményeket.

1.2. Az utasításban foglaltakat kell alkalmazni a minisztérium szervezeti egységei által folytatott adatkezelési műveletekre az adatok megjelenési formájától függetlenül, az adatkezelés teljes folyamatára kiterjedően - az adatok megszerzésétől vagy a minisztériumi szervnél történő keletkezésétől azok törléséig, illetve megsemmisítéséig -, függetlenül attól, hogy az adatok valamely nyilvántartási rendszer vagy valamely ügyben keletkezett irat részét képezik-e.

---

<sup>1</sup> Megjelent: Hivatalos Értesítő 2018/71.

<sup>2</sup> Hatályon kívül helyezve: 2010. évi CXXX. törvény 12. § alapján. Hatálytalan: 2019. I. 3-tól.

1.3. A minősített adatok kezelésére vonatkozó jogszabály eltérő rendelkezésének hiányában az utasítást kell alkalmazni a minősített adathordozóban szerepeltetett személyes adatok kezelése során.

## 1. Értelmező rendelkezések

2. Az utasítás alkalmazásában:

a) *adatgazda*: aki az adott adatkezelésre vonatkozó döntési jogosultsággal rendelkezik, elsődlegesen az érintett adatkezelő legkisebb önálló szervezeti egységének vezetője;

b) *adatkezelő szerv*: Belügyminisztérium;

c) *adatkezelő szerv vezetője*: miniszter;

d) *adatkezelő szervezeti egység*: államtitkárság, helyettes államtitkárság, főigazgatóság, Nemzeti Biztonsági Felügyelet, valamint az Ellenőrzési Főosztály, a Kommunikációs Főosztály és a Miniszteri Kabinet;

e) *információbiztonsági felelős*: a Belügyminisztérium Informatikai Biztonsági Szabályzatáról szóló BM utasítás szerinti felelős;

f) *egységes elektronikus adatvédelmi nyilvántartás*: a minisztériumi adatkezelő szervek által végzett adatkezelési tevékenységeket összesítő egységes nyilvántartás;

g) *közös adatkezelés*: olyan adatkezelés, amely esetében a minisztériumi adatkezelő szerv a feladatkörébe tartozó adatkezelés céljait és eszközeit más adatkezelő szervvel közösen határozza meg, így különösen a közös elektronikus információs rendszer vagy adatkezelési felület alkalmazása;

h) *tájékoztatás*: adatvédelmi incidens gyanújáról szóló bejelentés a minisztérium valamely szervezeti egysége részére, amely bárkitől származhat;

i) *Ügyfélszolgálat*: a minisztérium ügyfélszolgálati tevékenységét ellátó Személyügyi Helyettes Államtitkárság Titkársága Civilkapcsolati és Ügyfélszolgálati Osztály.

## II. FEJEZET

### RÉSZLETES RENDELKEZÉSEK

#### 2. Az adatkezelő szerv vezetőjének feladatai

3. Az adatkezelő szerv vezetője az általa vezetett adatkezelő szerv vonatkozásában felel:

a) az adatvédelmi és adatbiztonsági intézményrendszer kiépítéséért és működtetéséért;

b) a személyes adatok védelméhez és az információszabadsággal kapcsolatos követelmények érvényesüléséhez szükséges személyi, tárgyi és technikai feltételek biztosítását célzó, hatáskörébe tartozó intézkedések meghozataláért;

c) az alárendelt személyi állomány adatvédelmi oktatásáért és rendszeres továbbképzéséért;

d) a rendszeres adatvédelmi ellenőrzésért, az ellenőrzés során esetlegesen feltárt hiányosságok vagy jogszabálysértő körülmények megszüntetéséért, a személyi felelősség megállapításához szükséges eljárás kezdeményezéséért, ennek érdekében a hatáskörébe tartozó eljárások lefolytatásáért;

e) az érintett jogainak gyakorlásához, valamint tájékoztatásához szükséges feltételek biztosításáért;

f) az adatvédelmi hatásvizsgálatok lefolytatásáért és rendszeres felülvizsgálatáért, valamint az ahhoz szükséges feltételek biztosításáért;

g) az adatvédelmi feladatok ellátására alkalmas adatvédelmi tisztviselő kijelöléséért, nevének és elérhetőségének a Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: Hatóság) részére történő bejelentéséért;

h) az adatvédelmi tisztviselő feladatainak végrehajtásához, a személyes adatokhoz és az adatkezelési műveletekhez való hozzáféréshez, valamint az adatvédelmi tisztviselő szakértői szintű ismereteinek fenntartásához szükséges feltételek és források biztosításáért;

i) az adatvédelmi tevékenységgel kapcsolatos közzétételi kötelezettség teljesítéséért;

j) a közérdekű adatokra és közérdekből nyilvános adatokra irányuló adatigénylések határidőben történő megválaszolásáért.

### 3. Az adatvédelmi tisztviselő

4. Az adatvédelmi tisztviselőt írásban jelöli ki az adatkezelő szerv vezetője. Adatvédelmi tisztviselőnek csak olyan személy jelölhető ki, aki a személyi biztonsági feltételeknek megfelel.

5. Nem lehet olyan személyt kijelölni adatvédelmi tisztviselőnek, aki az adatkezelő szervnél adatkezeléssel kapcsolatos döntések meghozatalára jogosult személynek a Polgári Törvénykönyvről szóló 2013. évi V. törvény 8:1. § 2. pontja szerinti hozzátartozója.

6. Az adatvédelmi tisztviselő nevééről és elérhetőségéről a minisztériumi foglalkoztatottakat tájékoztatni kell, valamint a Hatóság nyilvántartásába be kell jelenteni.

7. Az adatvédelmi tisztviselő számára feladatainak ellátása céljából, az ahhoz szükséges mértékben a minősítéssel védett iratokba betekinthet.

8. Az adatkezelő szerv vezetője biztosítja az adatvédelmi tisztviselő számára meghatározott feladata kapcsán eljárva a hozzáférést a feladatai végrehajtásához szükséges elektronikus rendszerekhez, iratokhoz, egyéb adathordozókhoz, valamint a szakmai ismeretei naprakészen tartásához szükséges feltételeket, jogosultságokat és erőforrásokat rendelkezésére bocsátja.

9. A minisztériummal bármely jogszabály alapján foglalkoztatási jogviszonyban álló személyek a személyes adatai kezeléséhez és jogai gyakorlásához kapcsolódó valamennyi kérdésben a hivatali út betartása nélkül, közvetlenül és egyszerű módon fordulhatnak az adatvédelmi tisztviselőhöz.

10. Az adatvédelmi tisztviselő az adatkezelő szervnél más feladatokat is elláthat, azonban az adatkezelő szerv köteles biztosítani, hogy ezekből a más feladatokból adódóan ne keletkezzen összeférhetetlenség, és az egyéb munkaköri feladatok ellátása nem veszélyeztetheti az adatvédelmi tisztviselői feladatok ellátását.

11.<sup>3</sup> Az adatvédelmi tisztviselő - a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről szóló (EU) 2016/679 európai parlamenti és tanácsi rendeletben (a továbbiakban: GDPR rendelet), továbbá az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvényben (a továbbiakban: Infotv.) foglaltakon kívül -

a) adatvédelmi ellenőrzési tervet készít, amelyet az adatkezelő szerv vezetője hagy jóvá;

b) az adatvédelmi ellenőrzési terv alapján, valamint azon kívül szükség szerint, különösen adatvédelmi incidens esetén, ellenőrzi az adatkezelő szervnél az adatvédelmi és adatbiztonsági követelmények teljesítését;

c) az adatkezelési előírások megsértőjét felhívja a jogszerű állapot haladéktalan helyreállítására, és - adatvédelmi érdek sérelme esetén - a hiányosságokat közvetlenül jelzi az adatkezelő szerv vezetőjének, indokolt esetben kezdeményezi a felelősség megállapításához szükséges eljárást;

---

<sup>3</sup> Megállapította: 7/2021. (V. 6.) BM utasítás 10. § (1). Hatályos: 2021. V. 7-től.

d) közreműködik az adatvédelmi incidens kivizsgálásában, és a vizsgálat eredménye alapján - a jogszabályi feltételek fennállása esetén - a közigazgatási államtitkár jóváhagyásával az adatvédelmi incidenst bejelenti a Hatóság részére, valamint vezeti a minisztérium adatvédelmi incidens-nyilvántartását;

e) koordinálja a minisztériumba érkező, közérdekű adat megismerésére irányuló igények teljesítését, valamint személyes adatot nem tartalmazó kimutatást vezet a közérdekű adat megismerésére irányuló, elutasított igényekről és az elutasítás indokairól, amelyekről tárgyév január 31-ig éves jelentésben tájékoztatja a Hatóságot, valamint

f) részt vesz a Hatóság által szervezett képzéseken.

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

12. Az adatgazda abban az esetben végez előzetes hatásvizsgálatot tervezett vagy folyamatban lévő adatkezelésnél, ha az adatkezelés valamely - különösen új technológiákat alkalmazó - típusa, figyelemmel annak jellegére, hatókörére, körülményére és céljaira, valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, vagy, ha az adatkezelés kockázatának és lényeges körülmény - különösen az adatkezelés technológiájának - megváltoztatása esetén.

13. Az adatgazda a kockázatelemzési feladata kapcsán kikérheti a tervezett illetve megváltozott adatkezelés által érintett személyek véleményét.

14. Az adatgazda a kockázatelemzési feladata kapcsán kikéri a döntés végrehajtásáért felelős szakterület, az elektronikus információs rendszer biztonságáért felelős szervezet vezetőjének vagy az elektronikus biztonságért felelős személynek és a rendszerek üzemeltetésében résztvevő szervezeteknek, valamint az adatvédelmi tisztviselőnek a véleményét. Ezt követően megválaszolja az 1. függelékben foglalt kérdéseket.

15. 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 hatásvizsgálat lefolytatása alóli mentesítést tartalmazó valamely jogszabályban meghatározott kivételi körbe tartozik, úgy ennek tényét az adatgazda írásban rögzíti.

16. Az adatgazda köteles az előkészített adatkezelés esetén a 2. függelék szerinti adatkezelési tevékenységek nyilvántartásról szóló dokumentumot, és a 3. és a 4. függelék szerinti adatbiztonsági és a felelősségi körökre vonatkozó adatlapot kitölteni, és azt az adatvédelmi tisztviselőnek megküldeni. Az adatvédelmi tisztviselő a megküldött dokumentumokat az adatkezelési tevékenységek nyilvántartásába bejegyzi.

17. Amennyiben az adatgazda 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 - a döntése alapjául szolgáló legfontosabb szempontokat írásban megjelölve - adatvédelmi hatásvizsgálat lefolytatását kezdeményezi az adatkezelő szerv vezetőjénél.

18. Az adatkezelő szerv vezetője az adatgazda javaslatára elrendeli az adatvédelmi hatásvizsgálat lefolytatását vagy írásban rögzíti mellőzésének okait, és az adatvédelmi tisztviselő kapcsolódó álláspontját. Az adatvédelmi hatásvizsgálat lefolytatásáig, vagy az annak elmaradásával kapcsolatos okok írásban történő rögzítéséig az adatkezelésről szóló döntés nem hozható meg.

19. Az adatvédelmi hatásvizsgálat lefolytatásában az adatkezelés által érintett személyek vesznek részt. Az adatvédelmi hatásvizsgálat lefolytatását az adatvédelmi tisztviselő támogatja. Az adatvédelmi hatásvizsgálat során keletkezett iratok az adatkezelő szerv döntését előkészítő adatokat tartalmaznak, ezért azokon „Nem nyilvános!” jelzést kell elhelyezni. Ha a hatásvizsgálat során kezelt adatok egy részének esetében azok minősítésére vonatkozó jogszabályi feltételek fennállnak, akkor az adatkezelő szerv vezetője dönt a szükséges iratok minősítéssel történő védelméről és annak szintjéről.

20. Az adatgazda és az adatkezelés által érintett személyek az adatvédelmi hatásvizsgálat eredményeiről minősített adatot nem tartalmazó, „Nem nyilvános!” jelzéssel ellátott összefoglaló jelentést készítenek az 5. függelék szerinti módszertani leírás alapján.

21. Az adatvédelmi hatásvizsgálatról szóló összefoglaló jelentést az adatkezelő szervezeti egység vezetője hagyja jóvá.

22. Az adatvédelmi tisztviselő a jelentés alapján az adatkezelést bevezeti az adatkezelési tevékenységek nyilvántartásába.

23. Ha az adatvédelmi hatásvizsgálat arra az eredményre jut, hogy a tervezett adatkezelés jelentette kockázat nem mérsékelhető a rendelkezésre álló technológiák és a végrehajtási költségek szempontjából ésszerű módon - vagy azt jogszabály kötelezően előírja -, akkor az adatkezelő szerv előzetes konzultációt kezdeményez a Hatóságnál.

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

24. Az érintettet megillető jogok gyakorlására az érintettek adatainak védelmét szolgáló adatbiztonsági követelményeket szem előtt tartva csak a kérelmező megfelelő azonosítása, illetve kérelme tartalmának hitelesítése esetén van lehetőség. Nem biztosítható ezen jogok gyakorlása különösen az elektronikus aláírással nem hitelesített, vagy a kérelmező személyének azonosítását nem biztosító elektronikus levél, valamint telefax útján érkezett kérelmek esetén. Elektronikusan benyújtott kérelem esetén a megfelelő azonosítás az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény 18. §-a szerint valósulhat meg.

25. Az adatkezelő szerv az érintett részére nyújtandó bármely értesítést és tájékoztatást könnyen hozzáférhető és olvasható formában, lényegre törő, világos és közérthetően megfogalmazott tartalommal teljesíti. Az adatkezelő szerv az információt írásban, elektronikus úton, illetve az érintett kérelmére szóban is megadhatja, amennyiben az érintett személyazonossága igazolt.

26. Az érintett hozzáférési jogának gyakorlása során a tájékoztatást és az adatról kért első másolatot díjmenetesen kell biztosítani, kivéve, ha az érintett kérelme - annak ismétlődő jellege vagy jogszabályban, illetve a Hatóság joggyakorlata értelmében - túlzó. Ez esetben - eltérő jogszabályi rendelkezés hiányában - az adatkezelő szerv jogosult ésszerű, a közérdekű adat iránti igény teljesítéséért megállapítható költségterítés mértékéről szóló jogszabály előírásai alapján a Belügyminisztérium Igazgatása Önköltségszámítási Szabályzat szerint megállapított mértékű díjat felszámítani.

27. Az érintett hozzáférési jogának gyakorlása során megküldött tájékoztatókról a szervezeti egységek anonim nyilvántartást vezetnek, amelyről minden év január 31-ig a 6. függelék kitöltésével jelentést küldenek az adatvédelmi tisztviselő részére.

## **6. Az adatkezelési tevékenységek nyilvántartása**

28. A minisztérium az adatkezelői nyilvántartást és az adatkezelési tevékenységek nyilvántartását elektronikusan az arra létrehozott elkülönített rendszerben kezeli, amely adatlapokból áll. Az adatkezelői nyilvántartást és az adatkezelési tevékenységek nyilvántartását az adatvédelmi tisztviselő vezeti. Az adatkezelői nyilvántartásba és az adatkezelési tevékenységek nyilvántartásába az adatkezelő szervezeti egység vezetője az alábbi adatokat küldi meg:<sup>4</sup>

a) az előkészített, megváltozott és megszűnt adatkezelések esetén a 2., 3., 4. függelékek szerinti adatokat,

b) hatásvizsgálat elvégzése esetén a 25. pont szerinti adatokat,

c) a jogszabályi rendelkezés alapján adatvédelmi hatásvizsgálattal kötelezően vizsgálandó adatkezelési tevékenységek esetében, csak abban az esetben szükséges a hatásvizsgálatot megküldeni, ha az adatkezelő a minisztérium.

29. A minisztérium központi honlapján közzétett adatkezelési és adatvédelmi tájékoztatókkal kapcsolatban a közzététellel érintett szervezeti egység kikéri az adatvédelmi tisztviselő véleményét.

## **7. Az adatigénylés és a lekérdezés során irányadó szabályok**

30. A minisztériumi szervezeti egység érintett előadója a szerv feladataihoz kapcsolódó egyes eljárások során az országos hatósági nyilvántartásokból vagy más célból kezelt adatbázisokból lekért vagy átvett, de az ügy szempontjából érdektelenné vált, vagy fel nem használt személyes adatok esetében köteles az ügyirat továbbítását, illetőleg irattárba helyezését megelőzően gondoskodni azok dokumentált törléséről, illetve megsemmisítéséről.

31. Az olyan elektronikus információs rendszernél, ahol az adatkezelés célja, az adatkezelést folytató személy azonosítása, valamint az adatoknak és az elvégzett műveleteknek a folyamatos és zárt rendszerben történő naplózása nem biztosított, a törvényi előírások teljesítése érdekében más módon - így különösen manuálisan vezetett lekérdezési napló vagy a nyilvántartásból történő lekérdezéshez alkalmazott információs rendszerben történő rögzítéssel - kell gondoskodni az adatkezelési művelet céljának dokumentálásáról.

## **8. Adattovábbítás**

32. A minisztériumi szervezeti egység az adattovábbítás feltételeinek meglétét minden egyes személyes adattal összefüggésben köteles ellenőrizni, így különösen azt, hogy az igényelt adatokra vonatkozóan az adatok kezelőjének minősül-e.

33. Adatvédelmi szempontból akkor tekinthető az adattovábbítás jogszerűnek, ha a személyes adatot kezelő szerv vagy személy jogosult annak továbbítására, az adattovábbítás címzettje (adatkérő) pedig rendelkezik az adat kezeléséhez szükséges joggal vagy az érintett írásos - a vonatkozó jogszabályi elvárásoknak megfelelő tartalmú - hozzájárulásával és az adatkérés célja mindezzel összhangban van. Az adattovábbítás feltételeinek megléte és a célhoz kötöttség a jogszerűség együttes követelménye.

34. Harmadik személy vagy szerv által benyújtott adattovábbítási kérelem elbírálása - a törvényben kötelezően előírt adattovábbítás esetét kivéve - az adatkezelő szerv vezetőjének vagy az általa kijelölt vezetőnek a hatáskörébe tartozik, amellyel kapcsolatban kikérheti az adatvédelmi tisztviselő véleményét. Az adatigénylés abban az esetben teljesíthető, ha az tartalmazza:

a) az adatigénylés célját, jogalapját;

---

<sup>4</sup> Módosította: 7/2021. (V. 6.) BM utasítás 10. § (5) a).

- 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.

35. Az adattovábbítás történhet kérelem alapján egyedi adatszolgáltatással, illetőleg - törvény ilyen tartalmú rendelkezése vagy erre vonatkozó megállapodás alapján - közvetlen hozzáférés biztosításával.

## **9. Adattovábbítási nyilvántartás**

36. Ha olyan adat továbbítására kerül sor, amellyel kapcsolatban az adattovábbítást végző minisztériumi szervezeti egység - a GDPR rendelet, vagy Infotv. által biztosított jogait érintő - adatkezelési korlátozást jelzett, az adatkezelési korlátozást szerepeltetni kell az adattovábbítási nyilvántartásban.

37. Az olyan elektronikus információs rendszerek esetében, ahol a folyamatos és zárt rendszerben történő naplózás nem biztosított, valamint manuális adatkezelések esetén az adatkezelés célját, az érintett adatokat, illetve az adatkezelést folytató személy azonosítását lehetővé tevő adatokra és az elvégzett műveletekre vonatkozóan papíralapú adattovábbítási nyilvántartás vezetéséről kell gondoskodni.

## **10. A közvetlen lekérdezés**

38. A közvetlen lekérdezést biztosító rendszert - a lekérdezés és a felhasználás jogszerűségének dokumentálása érdekében - úgy kell kialakítani, hogy:

- a) a személyes adatokhoz történő hozzáférés egyedi azonosító és jelszó megadásához kötötten történjen;
- b) a lekérdezés naplózása biztosított legyen;
- c) a hozzáférésre felhatalmazott munkatárs a lekérdezéskor a rendszer erre a célra kialakított állományában rögzíteni tudja az adatkérés céljára utaló adatot, így különösen az ügyszámot.

## **III. FEJEZET**

### **AZ ADATVÉDELMI INCIDENSKEZELÉSI ELJÁRÁSREND**

#### **11. Az adatvédelmi incidens észlelése**

39. A minisztérium adatkezelésében és az adatfeldolgozónál bekövetkezett adatvédelmi incidens gyanúját észlelő személynek a tájékoztatást az adatgazdához, amennyiben az elektronikus információbiztonság körében következett be, az információbiztonságáért felelős szervezeti egység vezetőjéhez kell megtenni. A tájékoztatásnak, amennyiben lehetséges a 7. függelék szerinti adatokat kell tartalmaznia.

40. A minisztérium ügyfélszolgálatára külső észlelő személytől származó a minisztérium adatkezelésére vagy az adatfeldolgozóra vonatkozó adatvédelmi incidens gyanújának tárgyában érkezett tájékoztatást az Ügyfélszolgálat haladéktalanul továbbítja a feladat és hatáskörrel rendelkező adatfeldolgozó szervezeti egysége és a Minisztérium információbiztonságért felelős szervezeti egység vezetőjének és az adatvédelmi tisztviselőnek.

41. Ha a minisztérium ellenőrzésre jogosult szervezeti egysége a feladata ellátása során adatvédelmi incidens gyanúját észleli, haladéktalanul értesíti az érintett adatkezelő szervezeti egység vezetőjét, és a minisztérium információbiztonságért felelős szervezeti egység vezetőjét.

42. A minisztérium információbiztonságért felelős szervezeti egység vezetője az információbiztonsági felelős véleményének kikérése mellett megvizsgálja, hogy:

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

43. A minisztérium információbiztonságért felelős szervezeti egység vezetője - amennyiben az incidens gyanúja felmerül - a döntés előkészítésére szolgáló anyagot a megküldi az adatkezelő szervezeti egység vezetője számára. Ha az adatkezelő szervezeti egység vezetője nem állapítható meg, akkor az üzemeltetést végző szervezet az incidenskezelési eljárásnak megfelelően jár el.

44. Ha nem állapítható meg adatvédelmi incidens, de egyéb incidens bekövetkezése igen, akkor a feladat és hatáskört figyelembe véve kerül sor a további eljárás folytatására.

45. Az adatgazda vizsgálja a feladat és hatáskörébe tartozó nem informatikai rendszert érintő adatvédelmi incidens gyanújával érintett tájékoztatásokat.

## **12. A tájékoztatás megvizsgálása és az adatvédelmi incidens kezelése**

46. Ha az adatvédelmi incidens a rendelkezésre álló adatok alapján egyértelműen megállapítható az adatgazda, a 7. függelék szerinti bejelentett adatokat megküldi az adatvédelmi tisztviselőnek, aki 72 órán belül intézkedik a hatósági nyilvántartásba való bejelentésről.

47. Ha a rendelkezésre álló adatok alapján az adatgazda egyértelműen nem tudja megállapítani az adatvédelmi incidens bekövetkezését, de feltételezhető, hogy az esemény magas kockázattal járt az adatvédelmi tisztviselő véleményének megkérése mellett haladéktalanul összehívja az alábbi tagokból álló adatvédelmi incidens bizottságot (a továbbiakban: bizottság):

- a) adatvédelmi tisztviselő;
- b) információ biztonsági felelős;
- c) ellenőrzésre jogosult szervezeti egység, az Ellenőrzési Főosztály tagja;
- d) érintett adatgazda szervezeti vezetője;
- e) kommunikációs szervezeti egység, a Kommunikációs Főosztály tagja;
- f) informatikai feladatokat ellátó szervezeti egység, az Informatikai Főosztály vezetője.

48. A vizsgálat az adatvédelmi tisztviselő véleményének, szakértői tanácsának kikérésével és annak figyelembevételével történik.

49. A bizottság a tájékoztatást megvizsgálja, a tájékoztatótól valamint az adatfeldolgozótól szükség esetén további adatszolgáltatást kér, amelyet az érintettek kötelesek haladéktalanul teljesíteni. A bizottság gondoskodik az elsődleges intézkedések megtételéről. Ha a vizsgálat során a bizottság megállapítja az érintettek jogaival és szabadságaival kapcsolatban a magas kockázat fennállását, akkor a 7. függelék szerinti adatokat az adatvédelmi tisztviselő közreműködésével a Hatóság részére 72 órán belül megküldi az erre rendszeresített elektronikus felület igénybevételével.

50. Az adatvédelmi incidens bekövetkezése esetén a bizottság döntése alapján a minisztérium kommunikációs szervezeti egységének tagja tájékoztatja a 8. függelékben meghatározott adatokról az incidenssel érintetteket.

51. Az adatvédelmi tisztviselő a bizottság vagy az adatgazda által megküldött 7. függelék szerinti adatvédelmi incidenst bevezeti a minisztérium 9. függelék szerinti adatvédelmi incidens nyilvántartásba.



## IV. FEJEZET

### KÖZÉRDEKŰ ADATOK

#### **13. A közérdekű adatok megismerésére irányuló igény elintézésének eljárási szabályai és a költségtérítés**

52.<sup>5</sup> A közérdekű adat megismerésére irányuló igényt soron kívül be kell mutatni az adatkezelő szervezeti egység vezetőjének, aki haladéktalanul írásban értesíti az Jogtanácsosi és Adatvédelmi Főosztály (a továbbiakban: JAFO) vezetőjét. Az adatkezelő szervezeti egység vezetője köteles gondoskodni a válasz határidőben történő előkészítéséről. Az előkészített adatokat 8 napon belül meg kell küldeni a JAFO vezetőjének, aki az Infotv. szabályai alapján gondoskodik a válasz kiküldéséről.

53.<sup>6</sup> A közérdekű adat megismerése iránti igénynek a JAFO vezetője és az adatot kezelő szervezeti egység vezetője az igény tudomására jutását követő legrövidebb idő alatt, legfeljebb azonban 15 napon belül köteles eleget tenni.

54.<sup>7</sup> Ha a közérdekű adatot kezelő szerv javaslata alapján a JAFO az igény megtagadja, arról annak indokaival együtt 15 napon belül írásban vagy - ha elektronikus levelezési címét közölte - elektronikus úton értesíti az igénylőt az Infotv. alapján őt megillető jogorvoslati lehetőségekről való tájékoztatással együtt.

55. Ha az igényelt adat kezelője a minisztérium irányítása vagy felügyelete alatt álló szerv és egyértelműen megállapítható adatkezelői minősége, úgy az igényt a minisztérium haladéktalanul köteles továbbítani a közérdekű adatot kezelő szervnek. Az igény áttételéről egyidejűleg írásban tájékoztatni kell az igénylőt.

56.<sup>8</sup> Ha az igény 15 nap alatt nem teljesíthető, erről az igénylőt a JAFO vezetője - az adatokat kezelő érintett szervezeti egység vezetőjének tájékoztatása mellett - 15 napon belül írásban tájékoztatja.

57.<sup>9</sup> Ha az igénylés olyan adatra vonatkozik, amelyet az Európai Unió valamely intézménye vagy tagállama állított elő, a JAFO vezetője haladéktalanul megkeresi az Európai Unió érintett intézményét vagy tagállamát az Európai Unió és Nemzetközi Helyettes Államtitkárság, valamint a Miniszterelnökség feladat- és hatáskörrel rendelkező államtitkársága bevonásával, és erről az igénylőt tájékoztatja. A tájékoztatás megtételétől az Európai Unió érintett intézménye vagy tagállama válaszáig az adatkezelőhöz való beérkezéséig terjedő időtartam az adatigénylés teljesítésére rendelkezésre álló határidőbe nem számít bele.

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

---

<sup>5</sup> Módosította: 7/2021. (V. 6.) BM utasítás 10. § (5) b), c).

<sup>6</sup> Módosítva: 7/2021. (V. 6.) BM utasítás 10. § (5) d) alapján.

<sup>7</sup> Módosítva: 7/2021. (V. 6.) BM utasítás 10. § (5) d) alapján.

<sup>8</sup> Módosította: 7/2021. (V. 6.) BM utasítás 10. § (5) d).

<sup>9</sup> Módosítva: 7/2021. (V. 6.) BM utasítás 10. § (5) d) alapján.

59. A költségtérítés megállapításánál a közérdekű adat iránti igény teljesítéséért megállapítható költségtérítés mértékéről szóló 301/2016. (IX. 30.) Korm. rendelet szerinti költségelemek vehe-tők figyelembe.

60. A dologi és személyi költségek megállapításáról a számítási módjáról a Belügyminisztéri-um Igazgatása Önköltségszámítási Szabályzata rendelkezik.

61. Az adatigény teljesítésénél elszámolható költségek megállapítására minden esetben sor ke-rül az adatokat kezelő szervezeti egységnél a 10. függelékben feltüntetett dokumentum kitöltésé-vel, számlázásra azonban csak akkor kerül sor, ha ez indokolt és a teljesítéshez szükséges mun-kaerő-ráfordítás időtartama meghaladja a 4 munkaórát, vagy a dologi költségek vonatkozásában a másolt oldalak száma meghaladja a 10 oldalt. A személyi és dologi költségekről a minisztérium állít ki számviteli bizonylatot.

62.<sup>10</sup> A JAFO vezetője az adatigény megválaszolásában érintett szervezeti egység vezetőjének megküldi a 10. függelékben meghatározott dokumentumot az adatigénnyel együtt.

63. Az érintett szervezeti egység vezetője a közérdekű adatigényben foglaltak alapján előzete-sen felméri a kezelésében lévő adatok kiadására fordított munkaórát, amelyet kerekítve, az egyes munkafolyamatot végző dolgozó nevének, beosztásának feltüntetésével a 10. függelék szerinti dokumentumban rögzít.

64. Ha a személyi költségek a 4 munkaórát vagy a dologi költségek vonatkozásában a máso-landó oldalak száma a 10 oldalt meghaladja, e-mailben az igényelt közérdekű adatot kezelő szer-vezeti egység vezetője megküldi a 10. függelék szerinti dokumentumot a Pénzügyi Erőforrás-gazdálkodási Főosztály (a továbbiakban: PEF) vezetőjének a költségszámítás elkészítése céljából.

65.<sup>11</sup> A PEF vezetője, a rendelkezésre álló tényleges személyügyi béradatok és dologi költsé-gek feltüntetése után, a 10. függelék szerinti dokumentumot megküldi a JAFO vezetőjének a költségek összegszerű kimutatásával.

66.<sup>12</sup> A JAFO vezetője a várható személyügyi és dologi kiadások összegéről a közérdekű adat megismerésére vonatkozó igény beérkezésétől számított 15 napon belül tájékoztatást küld az adatigénylő részére.

67. Az adatigénylőnek a költség megfizetésének elutasítására és a bírósághoz forduláshoz a tá-jékoztatás kézhezvételétől számított 30 nap áll rendelkezésére.

68. Ha az adatigénylő a tájékoztatásban foglaltakat elfogadja, a költség elfogadásától számított 15 napon belül köteles azt befizetni a minisztérium által írásban meghatározott folyószámlaszám-ra.

69. A minisztérium a számviteli bizonylat elkészítése céljából az adatigénylőnek - a költségek-ről szóló tájékoztatóval egy időben - megküldi a 11. függelék szerinti dokumentumot, amelyen az adatigénylő nevét és címét szükséges feltüntetni a számviteli bizonylat kiállítása céljából.

70. A minisztérium az adatigényre a választ az előzetes költségelszámolás elfogadását követő 15 napon belül köteles megküldeni.

71. Ha az adatigénylő az általa elfogadott költségtérítést nem fizeti meg, vagy a bíróság jogerős határozatában foglalt fizetési kötelezettségének nem tesz eleget, a minisztérium végrehajtási eljá-rást indít.

72.<sup>13</sup> A 10. függelékben rögzített költségek megfizetéséről a JAFO vezetője dönt az adat-igénnyel kapcsolatos összes körülmény mérlegelése után.

---

<sup>10</sup> Módosítva: 7/2021. (V. 6.) BM utasítás 10. § (5) d) alapján.

<sup>11</sup> Módosítva: 7/2021. (V. 6.) BM utasítás 10. § (5) d) alapján.

<sup>12</sup> Módosítva: 7/2021. (V. 6.) BM utasítás 10. § (5) d) alapján.

<sup>13</sup> Módosítva: 7/2021. (V. 6.) BM utasítás 10. § (5) d) alapján.

73. A költségtérítés megfizetésénél az adatigénylőtől a minisztérium a költségek előlegezését kérheti, ha a költség összege meghaladja az 5000 Ft-ot. A költség előlegezéséről és annak mértékéről az adatigénylőt előzetesen írásban tájékoztatni szükséges.

## **14. A közérdekű adatok elektronikus úton történő közzététele**

74. Az adatkezelő szervezeti egység vezetője az általános közzétételi, valamint a különös és az egyedi közzétételi listában meghatározott adatok továbbítása és állandó karbantartása érdekében belső adatfelelőst nevez ki. Az adatfelelős kinevezéséről nevének, elérhetőségeinek feltüntetésével az adatkezelő szervezeti egység vezetője e-mailben értesíti az adatvédelmi tisztviselőt az Utasítás hatálybalépést követő 30 napon belül. Új szervezeti egység létrejötte vagy az adatfelelős személyének megváltozása esetén a bejelentést 15 napon belül kell megtenni.

75. Az adatfelelős gondoskodik a kezelésében lévő közérdekű és közérdekből nyilvános adatok, adatbázisok, illetve nyilvántartások leíró adatainak hitelességéről és a továbbított adatok rendszeres frissítéséről.

76.<sup>14</sup> Az adatfelelős a közzétételre előkészített adatokat, vagy a külön internetes honlapon történő kötelező közzététel esetén a közzétételre szolgáló külön internetes honlap linkjét továbbítja a JAFO részére. A JAFO az adatokat és a linket az adatvédelem érdekében a közzététel szempontjából megvizsgálja, majd a minisztérium kommunikációval foglalkozó szervezeti egységének (a továbbiakban: adatfeltöltő) az elektronikus úton történő közzététel érdekében átadja. Az adatfeltöltő az adatokat a [www.kormany.hu](http://www.kormany.hu) internetes oldal megfelelő közzétételi egységébe kereshető formában feltölti. Az adatfeltöltő tölti fel a közérdekű adatokat is az egységes közadatkereső rendszerbe. Az adatfeltöltő az adatok közzétételéről tájékoztatja az adatfelelőst és a JAFO-t.

77.<sup>15</sup> Az általános közzétételi listát, valamint a közzeendő adatkörtől függően, szükség szerint a különös és az egyedi közzétételi listát minden szervezeti egység saját hatáskörben készíti el, és azt tárgyév április 15-ig továbbítja a JAFO részére. A közzétételi listával kapcsolatban az adatvédelmi tisztviselő - igény szerint - tanácsot ad. A különös és az egyedi közzétételi lista elkészítéséhez a Hatóság véleménye szükséges, amelyet a JAFO szerez be, kivéve a külön internetes honlapon történő kötelező közzététel esetét. A közzétételi kötelezettséget az általános, a különös és az egyedi közzétételi listák alapján külön elektronikus honlapon teljesítő szervezeti egység a közzététellel kapcsolatos véleménykérési és engedélyezési eljárást a Hatóságnál saját hatáskörben végzi, és ennek eredményéről tájékoztatja az adatvédelmi tisztviselőt.

77/A.<sup>16</sup> A külön internetes honlapon történő kötelező közzététel esetén a közzététel szabályait a közzétételi kötelezettséggel érintett szervezeti egység saját hatáskörben határozza meg, és erről, valamint a szabályokban bekövetkezett változásról hét napon belül tájékoztatja a JAFO-t. A külön internetes honlapon való közzétételre kötelezett szervezeti egység a közzétételi listát tárgyév április 15-ig továbbítja a JAFO részére. A külön internetes honlapon közzeendő adatok valós és aktuális tartalmát, rendelkezésre állását a közzétételre kötelezett szervezeti egység saját hatáskörben ellenőrzi, és az adatokat közzéteszi.

## **15. Statisztikai adatszolgáltatás**

---

<sup>14</sup> Megállapította: 7/2021. (V. 6.) BM utasítás 10. § (2). Hatályos: 2021. V. 7-től.

<sup>15</sup> Megállapította: 7/2021. (V. 6.) BM utasítás 10. § (2). Hatályos: 2021. V. 7-től.

<sup>16</sup> Beiktatta: 7/2021. (V. 6.) BM utasítás 10. § (3). Hatályos: 2021. V. 7-től.

78. A minisztérium mint a Hivatalos Statisztikai Szolgálat tagja által előállított, az Országos Statisztikai Adatfelvételi Program kötelező adatszolgáltatásairól szóló 388/2017. (XII. 13.) Korm. rendelet szerinti adatokra vonatkozó, a minisztériumhoz érkező statisztikai adatkéréseket (a továbbiakban: statisztikai adatkérés) - függetlenül attól, hogy az adatkérő a megkeresésében milyen jogszabályra hivatkozik - az adott adat kezelésére kijelölt szervezeti egységhez kell továbbítani az adatkérés teljesítése érdekében. A minisztérium szervezeti egységénél felmerült statisztikai igény esetén, az adatigénylő statisztikai adatkérésével közvetlenül az adott adat kezelésére kijelölt szervezeti egységet keresi meg.

79.<sup>17</sup> A statisztikai adatkéréseket az e statisztikai adatkezelésre kijelölt szervezeti egység teljesíti

a) önállóan vagy

b) az adatkérő által megkeresett szervezeti egység útján, ha a statisztikai adatkérés az adatkérő adatigényének csak egy része volt.

Az adatkérésről és a teljesítéséről a JAFO-t tájékoztatni kell.

80. Ha a minisztériumhoz érkező adatkérés tartalma alapján nem állapítható meg egyértelműen, hogy a megkeresés statisztikai adatkérésnek minősül, vagy egyéb közérdekű adat megismerésére irányul, az adatkérést az adatvédelmi tisztviselő állásfoglalása szerinti szervezeti egység teljesíti.

81. A megkeresés teljesítése során törekedni kell arra, hogy az adatkérő az általa meghatározott határidőben választ kapjon. Ha ez valamilyen okból nem lehetséges, az adatkérőt erről tájékoztatni kell annak megjelölésével, hogy az adatszolgáltatást mikorra várhatja. Ha az adatkérő nem határozott meg határidőt, vagy az meghaladja a 15 napot, akkor legkésőbb 15 napon belül kell választ adni.

82. Az adatkezelő szervezeti egység által hivatalosan nyilvánosságra hozott statisztikai adatokon túlmenően más kiválogatási szempontú és rendezési elvű vagy részletesebb adatokra vonatkozó statisztikai adatkérés (a továbbiakban: egyedi statisztikai adatkérés) teljesítésével kapcsolatos költségek elszámolásának módjára a közérdekű adat iránti igény teljesítéséért megállapítható költségtérítés mértékéről szóló 301/2016. (IX. 30.) Korm. rendelet szerint a Belügyminisztérium Igazgatása Önköltségszámítási Szabályzatát kell alkalmazni. A költségjavaslatot a PEF ellenőrzi, szükség esetén korrigálja, arról számlát állít ki az adatkérő részére, és ezt eljuttatja az adatkérés teljesítéséért felelős szervezeti egység részére. A számlát az egyedi statisztikai adatkérés teljesítésével egyidejűleg kell az adatkérő részére megküldeni.

## V. FEJEZET

### OKTATÁS VIZSGÁZTATÁS

#### 16.<sup>18</sup> Követelmények

83.<sup>19</sup> A minisztérium állományába újonnan belépő foglalkoztatottak számára az adatvédelmi tisztviselő adatvédelmi oktatást tart.

84.<sup>20</sup> A minisztérium foglalkoztatottjai két évente elektronikus úton vagy személyesen részt vesznek az adatvédelmi tisztviselő által szervezett, adatvédelemmel és a közérdekű adatok nyil-

---

<sup>17</sup> Módosította: 7/2021. (V. 6.) BM utasítás 10. § (5) e).

<sup>18</sup> Megállapította: 7/2021. (V. 6.) BM utasítás 10. § (4). Hatályos: 2021. V. 7-től.

<sup>19</sup> Megállapította: 7/2021. (V. 6.) BM utasítás 10. § (4). Hatályos: 2021. V. 7-től.

<sup>20</sup> Megállapította: 7/2021. (V. 6.) BM utasítás 10. § (4). Hatályos: 2021. V. 7-től.

vánosságával kapcsolatos oktatáson, amely a közszolgálatban foglalkoztatottak számára jogszabályban előírt képzés keretében, az adatvédelemre és a közérdekű adatok nyilvánosságára vonatkozó PROBONO és BM RVTV portálon választható képzéssel is teljesíthető.

85.<sup>21</sup> Az általános adatvédelmi szabályok változásáról az adatvédelmi tisztviselő a minisztérium intranetes felületén ad tájékoztatást.

86.<sup>22</sup> A személyes adatot kezelő vagy személyes adat nyilvántartást vezető minisztériumi szervezeti egység a foglalkoztatottjai részére tárgyév augusztus 31-ig az adatkezelést meghatározó ágazati törvény szerinti oktatást biztosít, és az oktatás időpontjáról, tárgyköréről, a résztvevők létszámáról tárgyév szeptember 15-ig tájékoztatja a JAFO-t.

## 1. függelék

### Kérdőív az előzetes kockázatelemzéshez

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

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

Igen  Nem

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

Igen  Nem

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

Igen  Nem

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

Igen  Nem

b) Ha releváns szervezeti változás következik be:

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

Igen  Nem

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

Igen  Nem

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

- érint-e új vagy nagy létszámú érintett csoportot?

Igen  Nem

- rögzít-e ezen felül további személyes adatot?

Igen  Nem

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

Igen  Nem

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

Igen  Nem

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

---

<sup>21</sup> Megállapította: 7/2021. (V. 6.) BM utasítás 10. § (4). Hatályos: 2021. V. 7-től.

<sup>22</sup> Megállapította: 7/2021. (V. 6.) BM utasítás 10. § (4). Hatályos: 2021. V. 7-től.

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 eljárás-hoz 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. függelék

### Adatkezelési és adatfeldolgozó tevékenységek nyilvántartása

I. Adatkezelési tevékenységek nyilvántartása	
1. Az adatkezelés megnevezése:	
2. Az adatkezelő szerv neve és elérhetősége:	Belügyminisztérium Cím: 1051 Budapest, József Attila utca 2-4. Telefonszám: +36-1-441-1000
3. A közös adatkezelő és az adatkezelő szervezeti egység megnevezése	
4. Az adatvédelmi tisztviselő neve és elérhetősége:	
5. Az adatkezelés célja:	
6. Adatkezelés jogalapja:	
7. Az érintettek személyek köre:	
8. A személyes adatok kategóriái:	
9. A címzettek kategóriái:	
10. Harmadik országba történő adattovábbítás/harmadik ország vagy nemzetközi szervezet megnevezése:	
11. Az adatkezelési tevékenység törzési határideje:	
12. Adatok forrása:	
13. Az adatbiztonsággal összefüggő szervezeti és technikai intézkedések általános leírása:	Ennél a pontnál a következő jogszabályok alkalmazandók: 1. az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény, 2. az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet, 3. a Belügyminisztérium Informatikai Biztonsági Szabályzatáról szóló 19/2015. (VII. 31.) BM utasítás.
14. NAIH szám:	
15. Adatkezelési tájékoztató van-e? (Ha hozzájárulás a jogalap, feltétlenül szükséges készíteni.)	Lehetséges válaszok: 1. Nincs rá szükség, mert jogszabályi tájékoztatás van. 2. Nincs, azonban feltétlenül szükséges lenne.(Indoklás) 3. Igen van.
16. Elsődleges adattárolási hely: (ideértve az adatbiztonsági kockázatokat, javaslatokat is, ha vannak)	Ezen pont kitöltésénél az Informatikai Főosztály fog iránymutatást adni.
17. Vannak-e együtt tárolt adatok:	Igen/Nem.
18. Célhoz kötöttség elve érvényesül-e? Indoklással, szükség esetén javaslatl!	1. Igen, az 5. pontnak megfelelően. 2. Nem vagy csak részben. (Nem válasz esetén indoklás, javaslat szükséges.)
19. Adattakarékosság elve érvényesül-e? Indoklással, szükség esetén javaslatl!	1. Igen, a személyes adatok az adatkezelés céljának megfelelnek, relevánsak, és szükségesek. 2. Nem. (Nem válasz esetén indoklás, javaslat szükséges.)
20. Pontosság elve releváns, érvényesül-e? Indoklással, szükség esetén javaslatl!	1. Igen, a személyes adatok pontosak, naprakészek. 2. Nem. (Nem válasz esetén indoklás, javaslat szükséges.)
21. Korlátozott tárolhatóság elve érvényesül-e?	1. Igen, a személyes adatok kezelésére csak a cél eléréséhez szükséges ide-



nyesül-e? Indoklással, szükség esetén javaslatl!	ig kerül sor, amelyet jogszabály állapít meg. 2. Igen, a személyes adatok kezelésére csak a cél eléréséhez szükséges ideig kerül sor, amelyet az adatkezelő határoz meg. (Hozzájárulás esetén.) 3. A személyes adatok kezelésére közérdekű archiválás, tudományos és történelmi kutatás vagy statisztikai célból az eredeti adatkezelési céltól eltérő ideig kerül sor. (Az első kettővel is alkalmazható.) 4. Nem. (Nem válasz esetén indoklás, javaslat szükséges.)
22. Adatbiztonság elve érvényesül-e? Indoklással, szükség esetén javaslatl!	1. Igen, a személyes adatok megfelelő biztonsága biztosított. 2. Nem.(Nem válasz esetén indoklás, javaslat szükséges.)
23. Tájékoztatás megfelelő, tartalmazza valamennyi kötelező elemet? Indoklással, szükség esetén javaslatl!	1. A tájékoztatás a törvényi előírásnak megfelelő. 2. Az adatkezelés hozzájáruláson alapul. A tájékoztatás megfelelő. 3. Az adatkezelés nem az érintett hozzájárulásán alapul. A tájékoztatás megfelelő. 4. Az adatkezelés ..... alapul, tájékoztatás nincs/nem megfelelő. (Nem válasz esetén indoklás, javaslat szükséges.)
24. Törlés, elfeledtetés joga gyakorolható-e? Indoklással, szükség esetén javaslatl!	Ezek a jogok nem gyakorolhatóak, ha a jogalap jogi kötelezettség teljesítése, vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlás keretében végzett feladat végrehajtása. 1. Igen gyakorolható. 2. Nem. (Nem válasz esetén indoklás, javaslat szükséges.)
25. Korlátozás joga gyakorolható-e? Indoklással, szükség esetén javaslatl!	Az érintett ezzel a jogával a kötelező, és a hozzájáruláson alapuló adatkezelések esetében is élhet. A kötelező esetében csak akkor, ha az adatok pontosságát vitatja, a GDPR rendeletben szereplő felsorolás többi pontja szerint nem. 1. Igen. 2. Igen, de mivel az adatkezelés jogalapja jogszabályon alapul, csak az adatok pontosságát vitathatja. 3. Nem. (Nem válasz esetén indoklás, javaslat szükséges.)
26. Adathordozhatóság joga gyakorolható-e? Indoklással, szükség esetén javaslatl!	Csak a hozzájáruláson, vagy szerződésen alapuló adatkezelések esetén alkalmazható. További feltétel, hogy az adatkezelés automatizált módon történjen. Nem alkalmazható a közérdekű és a közhatalmi feladatok keretében végzett adatkezeléseknél! 1. Igen. 2. Nem. (Nem válasz esetén indoklás, javaslat szükséges.)
27. Tiltakozás joga gyakorolható-e? Indoklással, szükség esetén javaslatl!	Az érintett csak kivételes esetben! a közérdekű és a közhatalmi feladatok keretében végzett adatkezelések, és a jogos érdeken alapuló adatkezelések esetén élhet ezzel a joggal. [GDPR rendelet 6. cikk (1) e) és f) pont] 1. Igen, mert a jogalap .....! 2. Nem. (Nem válasz esetén indoklás, javaslat szükséges.)
28. Van-e adatfeldolgozási megállapodás az adatfeldolgozóval?	

### Gyakorlati útmutató:

1. Az adatkezelés megnevezése: A nyilvántartásban történő keresés lehetővé tétele céljából röviden kell megnevezni. A nyilvántartásnak az adatkezelést létrehozó törvény által meghatározott elnevezését kell megjelölni, amennyiben azonban rendelkezik egy általánosan használt fantázianévvel, akkor ezt az elnevezést is fel kell tüntetni. Az azonos adattartalommal rendelkező adatkezeléseket egységes elnevezéssel kell szerepeltetni.
2. Az adatkezelő nevét, címét, székhelyét, telefonszámát, e-mail-címét kell beírni.
3. Csak akkor kell kitölteni, ha van közös adatkezelő illetve van az adatkezelőnek képviselője.
4. A belső adatvédelmi felelős elnevezése május 25. napjától adatvédelmi tisztviselő lesz.
5. Az adatkezelés céljának rövid megfogalmazása.

6. Hozzájárulás vagy GDPR rendelet 6. cikk (1) bekezdésében foglalt jogalapok valamelyike.

Pontosan meg kell jelölni a fentieken kívül azt is, hogy milyen jogszabály (jogszabályhelyet is kérjük feltüntetni!) által meghatározott feladat teljesítése érdekében van erre szükség. Ilyen esetben a feladat meghatározást tartalmazó ágazati jogszabály megfelelő hivatkozási alapnak tekinthető.

7. Az érintettek kategóriái lehetnek: azon csoportok, amelyek tagjainak személyes adataival a Belügyminisztérium adatkezelést végez. Pl. az adatkezeléssel érintett személyek/nagykorú állampolgárok/gyermek, egyéni vállalkozók, gépjármű üzemben tartói stb.

8. Például: személyes adat, különleges adat, bűnügyi személyes adat, nemzeti adatvagyon, minősített adat.

9. Címzettek: akikkel a személyes adatot közölték, vagy közölni fogják, ideértve a harmadik országbeli címzetteket, vagy nemzetközi szervezeteket.

10. Harmadik ország: minden olyan ország, ami nem EU és EGT tag.

11. Ha jogszabály másképp nem rendelkezik, az adatokat az adatkezelés céljának elérésével, illetve az érintett kérésére törölni kell.

12. A kezelt adatok forrásának megjelölése (pl. érintett, más adatkezelőtől adatátvétellel).

Más adatkezelőtől történő adatátvétel esetén az adatokat továbbító adatkezelő adatvédelmi nyilvántartási számát is meg kell jelölni.

13. Lásd GDPR rendelet 32. cikk (1) bekezdése.

14. Ha az adatkezelés a NAIH részére már bejelentésre került.

II. Adatfeldolgozói tevékenységek nyilvántartása	
1. Az adatkezelés megnevezése:	
2. Az adatfeldolgozó(k) szervezeti egység megnevezése és elérhetősége(i):	
3. Az adatkezelési tevékenységek kategóriái:	
4. Adatvédelmi tisztviselő neve és elérhetősége:	
5. Harmadik országba történő adatátvitel/ harmadik ország vagy nemzetközi szervezet megnevezése:	
6. Az adatbiztonsággal összefüggő szervezeti és technikai intézkedések általános leírása:	
7. Elsődleges adattárolási hely: (ideértve az adatbiztonsági kockázatokat, javaslatokat is, ha vannak)	
8. Vannak-e együtt tárolt adatok:	
9. Célhoz kötöttség elve érvényesül-e? Indoklással, szükség esetén javaslattal!	
10. Az adattakarékosság elve érvényesül-e? Indoklással, szükség esetén javaslattal!	
11. Pontosság elve releváns, érvényesül-e? Indoklással, szükség esetén javaslattal!	
12. Korlátozott tárolhatóság elve érvényesül-e? Indoklással, szükség esetén javaslattal!	
13. Adatbiztonság elve érvényesül-e?	

Indoklással, szükség esetén javaslattal!	
14. Tájékoztatás megfelelő, tartalmazza valamennyi kötelező elemet? Indoklással, szükség esetén javaslattal!	
15. Törlés, elfeledtetés joga gyakorolható-e? Indoklással, szükség esetén javaslattal!	
16. Korlátozás joga gyakorolható-e? Indoklással, szükség esetén javaslattal!	
17. Adathordozhatóság joga gyakorolható-e? Indoklással, szükség esetén javaslattal!	
18. Tiltakozás joga gyakorolható-e? Indoklással, szükség esetén javaslattal!	
19. Ha adatfeldolgozók vagyunk, van-e adatfeldolgozási megállapodás az adatkezelővel?	

### 3. függelék

#### Felelősségi és feladatkörök meghatározása

	Nyilvántartás neve:	Név	Telefonszám	E-mail
1.	Döntéshozó személy az Adatkezelő (Helyettes Államtitkárság, Államtitkárság, Nemzeti Biztonsági Felügyelet) részéről:			
	Kapcsolattartó személy az Adatkezelő részéről:			
2.	Döntéshozó személy az Adatgazda (főosztály) részéről:			
	Kapcsolattartó személy az Adatgazda részéről:			
3.	Döntéshozó személy az Adatfeldolgozó részéről:			
	Kapcsolattartó személy az Adatfeldolgozó részéről:			

### 4. függelék

#### A személyes adatokat kezelő nyilvántartások adatbiztonsági felmérése (ADATLAP)

Az adatlap fókuszában a GDPR rendelet szerinti személyes adatokat kezelő nyilvántartások felmérése és a hatásvizsgálat elvégzésével összefüggésben a magas kockázatú adatkezelés megállapítása áll, a 29. cikk alapján létrehozott adatvédelmi munkacsoport (17/HU WP 248 rev.01) iránymutatásai alapján.

A személyes adatokat kezelő nyilvántartások adatbiztonsági felmérésének súlyponti kérdései a nyilvántartások bizalmassága sértetlensége és rendelkezésre állása oly módon, hogy a felmérés eredményei alapján megállapítható legyen, hogy az adatkezelés a GDPR rendelet alkalmazásában

„valószínűsíthetően magas kockázattal jár”-e, valamint a kockázatok kezelését célzó alkalmazott védelmi intézkedések és mechanizmusok (szervezeti intézkedések) biztosítják-e az érintettek és más személyek jogait és jogos érdekeit figyelembe vevő garanciákat.

A felmérés során számba vesszük, hogy az „adatkezelések” során jelenleg milyen személyi, adminisztratív, fizikai és elektronikus védelmi intézkedéseket alkalmaznak az adatbiztonsági kockázatok csökkentése érdekében.

Készült: 201.....-n a (adatkezelő szerv megnevezése) hivatalos helyiségében.

adatkezelő szerv megnevezése:

Ikt. szám:

Jelen vannak:

.....  
nyilvántartást kezelő szervezeti egység vezetője,

.....  
felmérést végző bizottság tagja,

.....  
felmérést végző bizottság tagja.

A NYILVÁNTARTÁS MEGNEVEZÉSE: .....

I. A NYILVÁNTARTÁS JELLEGÉNEK FELMÉRÉSE			
Felmérési kérdés	Igen/Van	Nem/Nincs	Megjegyzés
1. A nyilvántartás papíralapú.			
2. A nyilvántartás elektronikus.			
3. A nyilvántartáshoz kapcsolódik papíralapú adathordozó, amely személyes adatokat tartalmaz.			
4. A nyilvántartás alapja irodai alkalmazás (office termékek).			
5. A nyilvántartás alapja célszoftver (erre a célra fejlesztett speciális alkalmazás).			
II. A NYILVÁNTARTÁS SZEMÉLYI FELTÉTELEI			
Felmérési kérdés	Igen/Van	Nem/Nincs	Megjegyzés
6. A nyilvántartás kezelését az adatkezelővel (adatfeldolgozóval) munkaviszonyban álló személy(ek) kezeli.			
7. A nyilvántartásokat kezelő személy(ek) rendelkeznek egyéb személyi biztonságot fokozó ellenőrzéssel (erkölcsi bizonyítvány, nemzetbiztonsági ellenőrzés)?			
8. A nyilvántartást kezelő személy(ek) rendszeresen részt vesznek a nyilvántartások kezelésével összefüggő adatvédelmi és adatbiztonsági szabályokat feldolgozó továbbképzéseken?			
9. A nyilvántartást kezelő személy(ek) rendszeresen részt vesznek-e a nyilvántartások kezelésé-			

vel összefüggő adminisztratív (nyilvántartó rendszer) kezelési (iratkezelési) szabályok betartásával összefüggő képzéseken?			
<b>III. A NYILVÁNTARTÁS FIZIKAI BIZTONSÁGI FELTÉTELEI</b>			
Felmérési kérdés	Igen/Van	Nem/Nincs	Megjegyzés
10. A nyilvántartás és az azokhoz kapcsolódó személyes adatokat tartalmazó adathordozókhoz való illetéktelen (jogellenes) hozzáférést késleltető fizikai biztonsági eszközöket (beléptető rendszer, riasztó rendszer, biztonsági rács, biztonsági ajtó, páncélszekrény, zárható irodabútor) használnak.			
11. A nyilvántartás és az azokhoz kapcsolódó személyes adatokat tartalmazó adathordozók fizikai megsemmisülését megakadályozó biztonságtechnikai (tűzjelző, tűzálló páncélszekrény) rendszereket használnak.			
12. A nyilvántartást kezelő szervezeti egység objektumába a beléptetés ellenőrzött (beléptető rendszer, vendégnyilvántartás, csomagátvizsgálás) a portaszolgálatnál.			
13. A nyilvántartást kezelő szervezeti egységénél az objektumőrőség (portaszolgálat) 24 órás rendelkezésre állású.			
14. A nyilvántartást kezelő szervezeti egység irodái munkaidő után zártak, a kulcsdobozokat munkaidőn túl a portaszolgálatnál tárolják.			
15. A nyilvántartást kezelő szervezeti egység irodáiban a takarítás ellenőrzött körülmények között (személyes felügyelet mellett) történik.			
16. A nyilvántartást kezelő szervezeti egység nyilvántartásokat kezelő rendszerének perifériái (fénymásoló, nyomtató) munkaidőn túl nem elérhetőek (nem a folyosón vannak elhelyezve) az illetéktelenek és a jogellenes tevékenység végrehajtására készülő személyek számára.			
17. A nyilvántartást kezelő szervezeti egység feldolgozó helyiségébe a belépés ellenőrzött és illetéktelen személyek csak kísérettel (felügyelet mellett) tartózkodhatnak a helyiségben.			
<b>IV. A NYILVÁNTARTÁS ADMINISZTRATÍV BIZTONSÁGI FELTÉTELEI</b>			
Felmérési kérdés	Igen/Van	Nem/Nincs	Megjegyzés
18. A nyilvántartást kezelő szervezeti egységek (papíralapú vagy elektronikus) nyilvántartási rendszere alkalmas a személyes adatok nyomon követhető nyilvántartására.			
19. A nyilvántartás rekordjai, adategységei egyedi azonosítóval rendelkeznek.			
20. Az adatokhoz való hozzáférés (gyűjtés, módosítás, továbbítás) naplózott és a hiteles nyomon követés utólag is biztosított.			
21. A nyilvántartásból történő adatszolgáltatások (belső és külső átadások) naplózottak, utólag is hitelesen nyomon követhetőek.			

22. A nyilvántartás vezetésére használt (papír, elektronikus) rendszer/alkalmazás iratkezelési, vagy egyéb tanúsítvánnyal rendelkezik.			
<b>V. A NYILVÁNTARTÁS ELEKTRONIKUS BIZTONSÁGI FELTÉTELEI</b>			
Felmérési kérdés	Igen/Van	Nem/Nincs	Megjegyzés
23. A nyilvántartás elektronikus kezelését végző szervezet biztonsági szintbe (1-5) történő besorolása megtörtént.			
24. Az elektronikus nyilvántartás (elektronikus információs rendszer) legalább 3-as biztonsági osztályba történő besorolása megtörtént.			
25. A nyilvántartást biztosító elektronikus információs rendszer adatainak és naplóinak biztonsági mentése és a mentések biztonságos tárolása megoldott.			
26. A nyilvántartást biztosító elektronikus információs rendszer, rendelkezésre állása 24/7-es (folyamatos).			
27. A nyilvántartást biztosító elektronikus információs rendszer, rendelkezésre állása napi 8 órában, munkaidőben biztosított.			
28. A nyilvántartást biztosító elektronikus információs rendszer redundáns adattárolása, rendszerüzemeltetési környezete biztosított.			
29. A nyilvántartást biztosító elektronikus információs rendszer redundáns (szünetmentes) tápellátása biztosított.			
30. A nyilvántartás alapját képező elektronikus információs rendszerrel összefüggő hitelesítés és jogosultság ellenőrzés (autentikáció és autorizáció) biztosított.			
31. A nyilvántartást biztosító elektronikus információs rendszerben történő tranzakciók (felhasználói tevékenység) naplózottak.			
32. A nyilvántartást biztosító elektronikus információs rendszer biztonsági eseményei naplózottak.			
33. A naplófájlokat a biztonsági mentés tartalmazza.			
34. A nyilvántartást biztosító elektronikus információs rendszer biztonságos üzemeltetése hálózatzárolással szoftverrel biztosított.			
35. A nyilvántartást biztosító elektronikus információs rendszer biztonságos üzemeltetése adatlopás elleni védelemmel (szoftverrel) biztosított.			
36. A nyilvántartást biztosító elektronikus információs rendszer biztonságos üzemeltetése tűzfalvédelemmel biztosított.			
37. A nyilvántartások adatainak kezelése titkosított adathordozón (pl. BitLocker meghajtó titkosítás) történik.			

Kmf.

nyilvántartást kezelő szervezeti egység vezetője

felmerést végző bizottság tagja

felmerést végző bizottság tagja

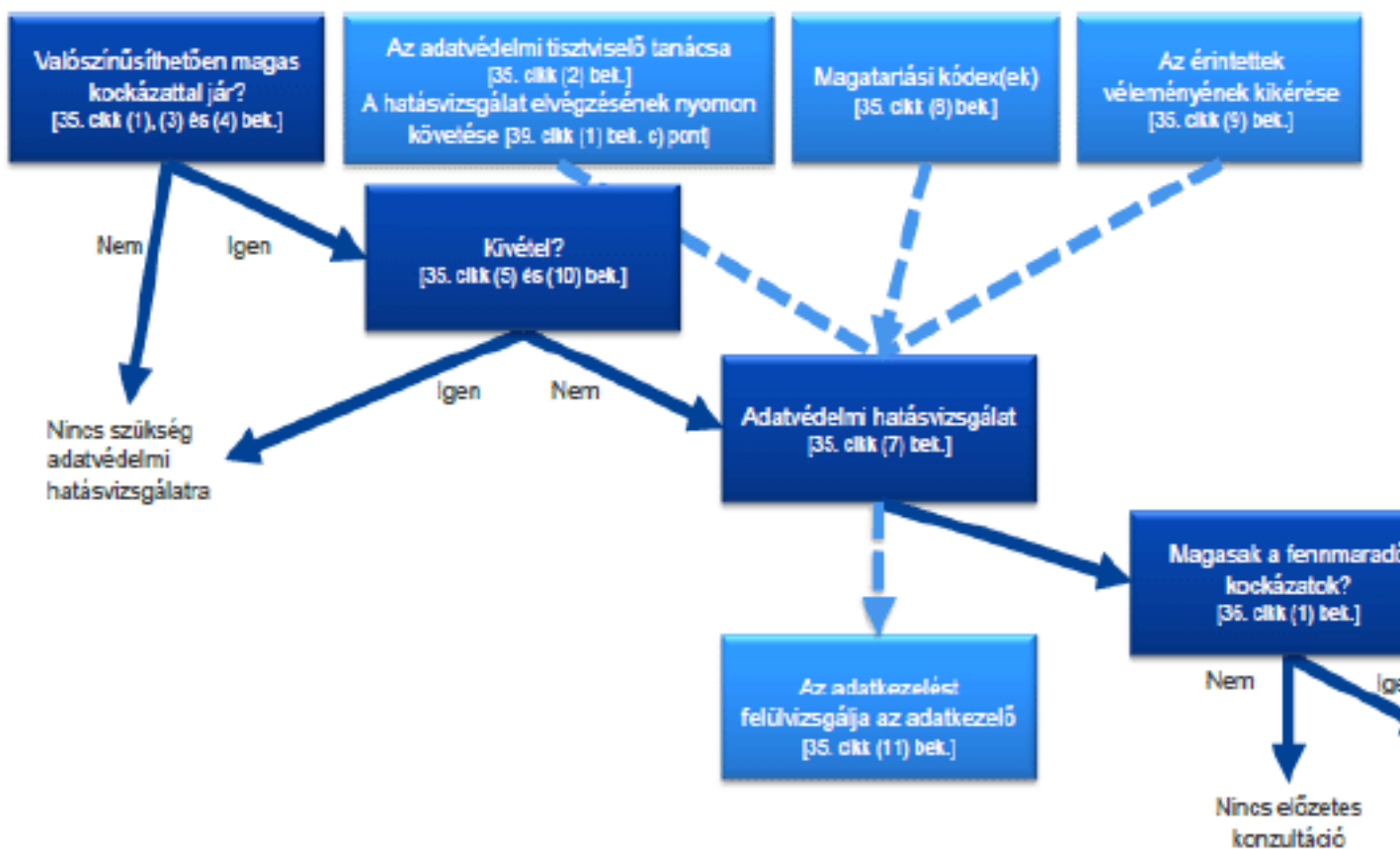
Készült: ..... példány/..... lap

Kapják:

## 5. függelék

### A hatásvizsgálat módszertana

1. Az alábbi ábra az általános adatvédelmi rendeletben az adatvédelmi hatásvizsgálattal kapcsolatosan megfogalmazott elveket szemlélteti:



2. A hatásvizsgálat lépéseinek bemutatása:



### 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;
- hatásvizsgálatra 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 lehetőségre. A tájékoztatás során ki kell térni az eljárás menetére, idejére, várt eredményére. Az esetleges konzultációt már a tervezési/fejlesztési szakaszban célszerű elvégezni, hogy az érintettek észrevételeit, ajánlásait esetlegesen implementálni lehessen, jelentős többletköltség nélkül. Az érintetti kör nincs korlátozva - a projekt tárgyát tekintve érintett lehet állami és civil szervezet, támogató, szolgáltató, fejlesztő és az adatkezelés adatalanyai egyaránt.

Az érintettek hatásvizsgálatba való bevonásának lehetőségei:

- az egyes érintett kategóriák meghatározása és párbeszéd folytatása az egyes kategóriák képviselőivel;
- konzultációs eljárások biztosítása, hogy az érintetteknek lehetőségük legyen álláspontjaik kifejtésére;
- a tervezet érintettek számára történő hozzáférhetővé tétele.

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

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

4.2. A lehetséges kockázatok csoportjai

- Személyeket érintő kockázatok:
  - az adatok nem megfelelő nyilvánosságra hozatala növeli annak esélyét, hogy olyan adatokat is megosztanak, amelyeket jogszerűen nem lehetne;
  - az adatkezelés célja megváltozhat, így az idő múlásával a tárolt adatokat másra használják fel az érintett tudta nélkül;
  - adatbázisok összefésülése, amelynek köszönhetően olyan felhasználói profilok hozhatók létre, amelyekből új információk nyerhetők ki;
  - azonosítók összekapcsolása, amely meggátolja az anonim felhasználást.
- Szervezeteket érintő kockázatok:
  - adatvédelmi hatóság álláspontjába vagy olyan jogszabályi előírásba való ütközés, amelynek következményeként
    - bírság vagy más szankciók is kiszabhatók;
    - olyan problémák felmerülése, amelyekre csupán a projekt elindítását követően derül fény, és a kijavításuk rendkívül költségigényes;
    - az adatminimalizálás elvébe ütköző felesleges, készletező, esetleg többszöri adatgyűjtés, amely így csökkentheti a projekt hatékonyságát;
    - a bizonytalan és nem megfelelő adatkezelés a társadalomban bizalomvesztést eredményezhet, amely bevételcsökkenés formájában jelenhet meg;
    - adatvesztés, amely az érintettek számára kárt okoz, valamint az érintettek részéről kártérítési igényt generál.
  - Jogi szabályozásnak való megfelelés vizsgálata:
    - az adatkezelés nem felel meg a tagállami hatóság állásfoglalásaiban foglaltaknak;
    - az ágazat-specifikus előírásoknak vagy
    - az alkotmányjogi előírásoknak.

#### 4.3. Az adatvédelmi kockázatok rangsorolása

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

- alacsony (esély van a kockázat megjelenésére, de vannak enyhítő körülmények);
- közepes (valószínű, hogy megjelenik a kockázat, ha nem történik korrekció);
- magas (megjelenik a kockázat, ha nem történik korrekció) szintű kockázat.

Egy kockázat mértékét négy tényező befolyásolja:

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

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

1. kis számú =1,
2. közepes =2,
3. nagy számú =3

érintett adatkezelését valósítja meg.

A kockázat elhárításának ügyviteli sürgőssége: a bejelentő nem itéli sürgősnek=1, a bejelentő sürgősnek itéli=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 bizalmasága 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 érten-dő 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, külön-böző célokból, illetve eltérő adatkezelők által végzett adatkezelési műveletből származó adatok-kal, 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 jogaikat gyakorolni. A kiszolgáltatott helyzetben lévő érintettek közé sorolhatók a gyermekek (ők úgy tekintendők, mint akik nem tudják tudatosan és átgondoltan ellenezni vagy engedélyezni adataik kezelését), a munkavállalók, a lakosság különleges védelmet igénylő, kiszolgáltatottabb helyzetben lévő rétegei (mentális betegségben szenvedők, menedékkérők vagy az idősek, betegek stb.), valamint az egyének minden olyan esetben, amikor az érintett és az adatkezelő közötti kap-csolatban 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, vala-mint 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 társa-dalmi következményei tehát beláthatatlanok lehetnek. Az adatvédelmi hatásvizsgálat révén az adatkezelő megismerheti és orvosolhatja az ilyen jellegű kockázatokat. Például bizonyos, a „dol-gok internetét” használó alkalmazások jelentős hatást gyakorolhatnak az egyének mindennapi életére és magánéletére, ezért szükségessé teszik az adatvédelmi hatásvizsgálat elvégzését.

- Azok az esetek, amikor az adatkezelés önmagában véve „megakadályozza, hogy az érintettek a jogaikat gyakorolják vagy szolgáltatásokat vegyenek igénybe vagy szerződést érvényesítse-nek”[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 művelet 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 - kezelési folyamat (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.

## 6. függelék

## Adatlap a szervezeti egységek részére az érintett jogainak gyakorlására vonatkozó kimutatóshoz

A kitöltő szervezeti egység:				
Az érintett saját adataira vonatkozó kérelmek:				
A kérelem jellege	Teljesített	Részben teljesített	Elutasított	
Tájékoztatás iránti kérelem saját nyilvántartott személyes adatról				
Tájékoztatás iránti kérelem arról, hogy az érintett személyes adatát kinek továbbították				
Helyesbítés iránti kérelem				
Törlés iránti kérelem				
Az érintett személyes adatára vonatkozó részben teljesített, illetve elutasított kérelmek indokolása:				
A közérdekű adatok megismerésére vonatkozó kérelmek:				
Teljesített	Részben teljesített	Elutasított		
A közérdekű adatok megismerésére vonatkozó részben elutasított kérelmek indokolása:				

### 7. függelék

#### Bejelentő lap az adatkezelő részére adatvédelmi incidens esetén

1. Az adatvédelmi incidenst bejelentő Tájékoztató adatai:

Név: .....

..

E-mail-cím: .....

Cím: .....

..

Telefonszám: .....  
szám: .....

Kapcsolattartó megnevezése, elérhetősége (telefonszám, e-mail):

.....

..

.....

..

.....

..

1.1. Az adatkezelőn kívüli felek részvétele az adatvédelmi incidenssel érintett szolgáltatásban.

1.2. Részt vesz-e az adatkezelőn kívül más az adatvédelmi incidenssel érintett szolgáltatásban:

.....  
..  
.....  
..  
.....  
..

1.3. Az adatkezelőn kívüli fél megnevezése és minősége:

.....  
..  
.....  
..  
.....  
..

2. Az adatvédelmi incidenssel kapcsolatos időpontok:

Kezdő időpont: .....

Záró időpont: .....

Az adatvédelmi incidens továbbra is fennáll: .....

Az incidensről való tudomásszerzés időpontja: .....

Az incidens észlelésének módja: .....

Az adatfeldolgozó általi értesítés időpontja: .....

A késedelmes tájékoztatás indokai:

.....  
..  
.....  
..  
.....  
..  
.....  
..  
.....  
..

Egyéb megjegyzések az incidens időpontját illetően:

.....  
..  
.....  
..  
.....  
..

.....  
..  
.....  
..

3. Az adatvédelmi incidens adatai (kérem, húzza alá a megfelelő választ, amennyiben szükséges fejtse ki a részleteket):

3.1. Sérülés jellege:

- bizalmas jelleg:
- integritás:
- rendelkezésre állás:

3.2. Az adatvédelmi incidens jellege (kérem, húzza alá a megfelelő választ, amennyiben szükséges fejtse ki a részleteket):

- eszköz elvesztése vagy ellopása:
- informatikai rendszer feltörése (hackelés):
- papíralapú dokumentum nem megfelelő módon történő megsemmisítése:
- papíralapú dokumentum elvesztése, ellopása vagy olyan helyen hagyása, amely nem minősül biztonságosnak

- rosszindulatú számítógépes programok (pl. zsarolóprogram)
- elektronikus hulladék (a személyes adatok rajta maradnak az elavult eszközön):
- személyes adatok téves címzett részére történő küldése:
- levél elvesztése vagy jogosulatlan felnyitása
- adathalászat
- személyes adatok nagy nyilvánosság előtti jogellenes közzététele
- személyes adatok jogosulatlan szóbeli közlése
- egyéb: .....
- .....
- .....

4. Az adatvédelmi incidens okai (kérem, húzza alá a megfelelő választ, amennyiben szükséges fejtse ki a részleteket):

- szervezeten belüli, rosszhiszeműnek nem minősülő cselekmény (belső szabályzat megsértése által):

- szervezeten belüli, rosszhiszemű cselekmény:
- külső, rosszhiszeműnek nem minősülő cselekmény:
- külső, rosszhiszemű cselekmény:
- egyéb: .....
- .....
- .....

5. Az adatvédelmi incidenssel érintett személyes adatok köre:

5.1. Személyes adatok (kérem, húzza alá a megfelelő választ, amennyiben szükséges fejtse ki a részleteket):

- személyazonossághoz kapcsolódó adatok:



- elérhetőségi adatok:
- azonosító adatok:
- személyi szám:
- hivatalos okmányok:
- helymeghatározó adatok:
- gazdasági, pénzügyi adatok:
- büntetett előélettel, bűncselekményekkel vagy büntetéssel, intézkedéssel kapcsolatos adatok:
- különleges adatok:

5.2. Különleges adatok (legalább egy kiválasztása kötelező):

- faji eredetre, nemzetiséghez tartozásra vonatkozó adatok:
- politikai véleményre vonatkozó adatok:
- vallásos vagy más világnézeti meggyőződésre vonatkozó adatok:
- érdek-képviselési szervezeti tagságra vonatkozó adatok:
- szexuális életre vonatkozó adatok:
- egészségügyi adatok:
- genetikai adatok:
- biometrikus adatok:
- még nem ismert:
- egyéb: .....
- .....
- .....

5.3. Az adatvédelmi incidenssel érintett személyes adatok becsült száma: .....

6. Az érintettek jellege (kérem, húzza alá a megfelelő választ, amennyiben szükséges fejtse ki a részleteket):

- alkalmazottak:
- felhasználók:
- feliratkozók:
- diákok:
- katonai állomány tagjai:
- ügyfelek (jelenlegi és potenciális):
- páciensek:
- kiskorúak:
- kiszolgáltatott személyek:
- hatósági eljárás vagy intézkedés alá vont, vagy azok által érintett személyek:
- még nem ismert:
- egyéb: .....
- .....
- .....

6.1. Az incidenssel érintett adatalanyok részletes leírása (pl. adatbázisokban szereplő munkavállalók leírása):

.....  
 ..

.....  
..  
.....  
..

6.2. Az adatvédelmi incidenssel érintettek becsült száma: .....

7. Az incidens előtt alkalmazott intézkedések leírása (pl. tűzfal, vírusellenőrzés, adatszivárgás elleni védelmi rendszer):

.....  
..  
.....  
..  
.....  
..

8. Következmények:

8.1. Bizalmas jelleg sérülése: (kérem, húzza alá a megfelelő választ, amennyiben szükséges fejtse ki a részleteket)

- Szélesebb körű hozzáférés, mint ami szükséges, vagy amihez az érintett hozzájárult:
- Az adat összekapcsolhatóvá vált az érintett egyéb adatával:
- Az adatot más célokból történő, tisztességtelen módon történő kezelése lehetséges:
- egyéb: .....

.....  
.....

8.2. Integritás sérülése: (kérem, húzza alá a megfelelő választ, amennyiben szükséges fejtse ki a részleteket)

- Az adat módosíthatóvá vált annak ellenére, hogy archivált vagy elavult volt:
- Az adatot valószínűsíthetően módosították egyébként pontos adatokra, és azokat eltérő célokra használhatták:
- egyéb: .....

.....  
.....

8.3. Rendelkezésre állás sérülése: (kérem, húzza alá a megfelelő választ, amennyiben szükséges fejtse ki a részleteket)

- Az érintettek számára történő kritikus szolgáltatásnyújtás képességének módosulása:
- egyéb: .....

.....  
.....

8.4. Az érintetteket ért fizikai, anyagi vagy nem vagyoni károk, vagy egyéb jelentős következmények:

8.5. Az incidens valószínűsíthető hatásai az érintettek: (kérem, húzza alá a megfelelő választ, amennyiben szükséges fejtse ki a részleteket)

- személyes adatok feletti rendelkezés elvesztése:
- érintett jogainak korlátozása:
- hátrányos megkülönböztetés:
- személyazonosság-lopás:
- személyazonossággal való visszaélés:
- pénzügyi veszteség:
- álnevesítés engedély nélküli feloldása:
- jó hírnév sérelme:
- szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülése:
- egyéb: .....
- .....
- .....

8.6. A valószínűsíthető következmények súlyossága: (kérem, húzza alá a megfelelő választ, amennyiben szükséges fejtse ki a részleteket)

- elhanyagolható:
- korlátozott:
- jelentős:
- maximális:

9. Az incidens orvoslására megtett intézkedések:

9.1. Megtett intézkedések (az adatvédelmi tisztviselő vagy a bizottság tölti ki) A megtett védelmi intézkedések leírása:

.....

..

.....

..

.....

..

.....

..

9.2. Az érintettek tájékoztatása: (kérem, húzza alá a megfelelő választ, amennyiben szükséges fejtse ki a részleteket) A tájékoztatás tervezett időpontja:

- még nincsen eldöntve:
- a tájékoztatás hiányának indokai:
- tényleges ideje, tartalma:
- érintetteknek javasolt intézkedések:
- intézkedések leírása, amelyek alapján az érintettek tájékoztatásra nem került sor
- tájékoztatott érintettek száma:
- az érintett tájékoztatásának formája:
- az érintetteknek szóló tájékoztatás tartalma:
- nyilvánosan közzétett információk vagy hasonló intézkedés:

.....

..

.....  
..  
.....  
..  
.....  
..

10. Egyéb:

.....  
..  
.....  
..  
.....  
..  
.....  
..  
.....  
..  
.....  
..

11. Egyéb bejelentések:

.....  
..  
.....  
..  
.....

Más hatóságoknak (EU tagállami) vagy tagállamnak bejelentette-e az adatvédelmi incidenst?

.....  
..  
.....  
..  
.....

## 8. függelék

### Az érintett tájékoztatása az adatvédelmi incidensről (GDPR rendelet 34. cikk)

1. Az adatvédelmi incidens időpontja: .....

2. Jellege:

.....  
..

.....  
..  
.....  
..  
.....  
..  
.....  
..  
.....  
..  
.....  
..

3. Az adatvédelmi tisztviselő/kapcsolattartó neve:

.....  
..  
Elérhetősége:  
.....  
..

4. Az adatvédelmi incidensből eredő valószínűsíthető következmény(ek):

.....  
..  
.....  
..  
.....  
..  
.....  
..  
.....  
..  
.....  
..  
.....  
..

5. Az adatvédelmi incidens kezelésével kapcsolatban tervezett, illetve megtett intézkedések (ideértve a hátrányos következmények enyhítését célzó intézkedéseket):

.....  
..  
.....  
..  
.....  
..  
.....  
..

.....  
..  
.....  
..  
.....  
..

6. Az érintett számára javasolt intézkedések megtétele a bekövetkezett kár enyhítése érdekében:

.....  
..  
.....  
..  
.....  
..  
.....  
..  
.....  
..  
.....  
..  
.....  
..

## 9. függelék

### Az adatvédelmi incidensek nyilvántartása és bejelentése (GDPR rendelet 33. cikk)

1. Az Adatkezelő (Bejelentő adatai)

Név: .....

..

Ország: .....

szág: .....

Irányítószám és hely:

.....

..

Utca neve és száma:

.....

..

2. Az adatvédelmi tisztviselő/kapcsolattartó neve:

.....

..

Elérhetősége: .....

3. Az Incidens időpontja

Kezdete: .....

Tudomásra jutás időpontja:

.....  
..

4. Az incidens jellege

Az Incidens leírása (nem jár kockázattal, kockázattal jár, magas kockázattal jár):

.....  
..  
.....  
..  
.....  
..

5. Az incidensben érintett adatok

Az adatok kategóriáinak leírása (különleges, bűnügyi adatok kiemelése):

.....  
..  
.....  
..

6. Az incidensben érintett személyek kategóriái

Az érintettek csoportjának leírása:

.....  
..  
.....  
..  
.....  
..  
.....  
..

7. A megelőzésre tett védelmi intézkedések

Az incidens megelőzésére tett védelmi intézkedések rögzítése:

.....  
..  
.....  
..  
.....  
..  
.....  
..

8. Az incidens következményei

Az érintettre gyakorolt bekövetkezett hatások leírása (fizikai, vagyoni, nem vagyoni):

.....  
..

.....  
..  
.....  
..  
.....  
..

9. Az Incidens valószínűsíthető következményei

Az érintettre gyakorolt lehetséges hatások leírása (fizikai, vagyoni, nem vagyoni):

.....  
..  
.....  
..  
.....  
..  
.....  
..

10. Megtett intézkedések

A megtett védelmi intézkedések leírása:

.....  
..  
.....  
..  
.....  
..  
.....  
..

Az érintettek tájékoztatása (tájékoztatás ideje, tartalma, érintetteknek javasolt intézkedések):

.....  
..  
.....  
..  
.....  
..

Egyéb:

.....  
..  
.....  
..  
.....  
..



## KIMUTATÁS

A közérdekű adat megismerésére vonatkozó igénnyel kapcsolatos költség előzetes és utólagos elszámolásához, munkaidő-elszámoláshoz  
a BM/.....-...../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:

PEF 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			

ma			
	A/3		

Feladatvégzéshez igénybe vett adathordozók száma: ..... db

A feladat elvégzését követően az ügyintéző aláírása:	
A feladat elvégzését igazoló vezető aláírása:	

4.<sup>23</sup> Tényleges költségek kimutatása:

Pénzügyi/személyügyi szervezeti egység bérkimutatása (óra/Ft) Dologi ség: ..... Személyi költség: ..... Összesen: .....	
Pénzügyi vezető aláírása:	
Minden ügyintéző külön munkaidő-elszámolást tölts ki.	
A kitöltött és aláírt elszámolást a Jogtanácsosi és Adatvédelmi Főosztályra kell elektroniku- san megküldeni.	

## 11. függelék

Az Infotv. 28. § (2) bekezdése alapján az igénylő személyes adatai a költségtérítés  
megfizetése érdekében

A közérdekű adat megismerésére vonatkozó igény tárgya:

.....

..

Az igénylő

Neve: .....

ve: .....

Címe: .....

Adóazonosító jele/adószáma: .....

Számlázásra vonatkozó adatok

Számlázási név: .....

Számlázási cím: .....

Kelt ....., ..... év ..... hó ..... nap

.....

aláírás

Az Ön személyes adatait a Belügyminisztérium mint adatkezelő a számviteli bizonylat kiállításához használja fel. Az adatkezelés idejére és az adatok átadásának szabályaira a pénzügyi bizonylatok megőrzésére és ellenőrzésére vonatkozó törvényi előírások az irányadóak. A Belügy-

<sup>23</sup> Módosította: 7/2021. (V. 6.) BM utasítás 10. § (5) f).

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