MAGYAR HONVÉDSÉG
KIBERMŰVELETI PARANCSNOKSÁG

A MAGYAR HONVÉDSÉG

KIBERMŰVELETI PARANCSNOKSÁG PARANCSNOKÁNAK

12/2023 MH KIBPK **MH KIBP PK**

I N T É Z K E D É S E

Adatvédelmi, Adatbiztonsági és Közérdekű adatok kezelésére vonatkozóan

2023.

TARTALOMJEGYZÉK

1. Általános rendelkezések

Jelen intézkedést a kapcsolódó Európai Unió jogával, a nemzeti jogszabályokkal, közjogi szervezetszabályozó eszközökkel és belső rendelkezésekkel együtt kell alkalmazni azzal, hogy a honvédelmi adatkezelésekről szóló 2022. évi XXI. törvény hatálya alá tartozó adatkezelések tekintetében az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.), a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet) szóló az Európai Parlament és a Tanács (EU) 2016/679 rendelete (a továbbiakban: EU rendelet) hatálya alá tartozó adatkezelések vonatkozásában az EU rendelet és az Infotv. vonatkozó rendelkezéseit kell alkalmazni.

Az intézkedést szükség szerint, de legalább évente – legkésőbb december 01-ig – felül kell vizsgálni. A felülvizsgálatot a Magyar Honvédség Kiberműveleti Parancsnokság (a továbbiakban: MH KIBP) adatvédelmi tisztviselője végzi el, a felülvizsgálat tényét feljegyzésben rögzíti.

2. Az intézkedés hatálya

Az intézkedés személyi hatálya az MH KIBP és a Magyar Honvédség Kiber- és Információs Műveleti Központ (a továbbiakban: MH KIMK) teljes személyi állományára kiterjed.

Jelen intézkedést az MH KIBP és MH KIMK tevékenysége során keletkező közérdekű adatokra, közérdekből nyilvános adatokra és a személyes vagy különleges adatokhoz kapcsolódó adatkezelésekre – ideértve az adatfeldolgozást – is alkalmazni kell.

Az intézkedés hatálya kiterjed minden, az adatkezelés során felhasznált tárgyi eszközre, függetlenül annak üzemelési helyétől, valamint azokra a helyiségekre és külső helyszínekre, ahol adatkezelés vagy adatfeldolgozás történik.

3. Az intézkedés célja

Az intézkedés célja, hogy meghatározza:

a) azokat a szabályokat, eljárásrendeket, melyek a személyes adatok kezelése során a természetes személyek jogainak és szabadságainak védelme érdekében szükségesek;

b) az MH KIBP és MH KIMK tevékenységéhez kapcsolódó személyes adatok kezelésének feltételeit és céljait, támogassa az érintettek magánszférájának tiszteletben tartását és az adatvédelmi tudatosságot;

c) a vonatkozó eljárásrendet, melyek garantálják az MH KIBP és MH KIMK feladatainak ellátása során keletkező közérdekű adatok nyilvánosságához, megismeréséhez fűződő alapvető jog érvényre juttatását.

4. Értelmező rendelkezések

Az intézkedés alkalmazása során az EU rendeletben, valamint az Infotv-ben rögzített fogalmakat kell alkalmazni.

Az előző bekezdésben meghatározottakon túl, az intézkedés alkalmazásában:

a) *bizalmasság:* az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény 8. § (1) bekezdés 8. pontja alapján, az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról;

b) *harmadik fél:* EU rendelet 4. cikk 10. pont értelmében, az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely nem azonos az érintettel, az adatkezelővel, az adatfeldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére felhatalmazást kaptak;

c) *közérdekű adat:* Infotv. 3.§ 5. pont alapján, az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő és tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől, így különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre, annak eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat;

d) *közérdekből nyilvános adat:* Infotv. 3.§ 6. pont alapján, a közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli;

5. Adatkezelő

Az adatkezelő megnevezése: Magyar Honvédség Kiberműveleti Parancsnokság
Székhelye: 2000 Szentendre, Dózsa György út 12-14.
Telephelyei: Budapest (HM-II. objektum, 1135 Budapest, Lehel utca 35-37.)
Székesfehérvár, Alba Regia laktanya, 8000 Székesfehérvár, Mészáros Lázár u. 2.
Postacíme: 1885, Budapest, Pf. 25.
Telefonszáma: 0622/542-811, 061/236-5262
e- mail címe: szerv.mh.kibp@mil.hu
Jogállása: közfeladatot ellátó szerv

Az adatkezelő vezetője és egyben képviselője: Magyar Honvédség Kiberműveleti Parancsnokság parancsnoka (a továbbiakban: parancsnok).

Az adatkezelő képviselőjének feladata az adatvédelmi és az információszabadsággal kapcsolatos tevékenység felügyelete, a szükséges erőforrások biztosítása, a megfelelő szabályozók kiadása.

6. Adatvédelmi tisztviselő

Az MH KIBP Jogi és Igazgatási Alosztály személyi állományából adatvédelmi tisztviselő kerül kijelölésre az MH KIBP és MH KIMK adatvédelmi feladatainak ellátására. Az adatvédelmi tisztviselő ezen tevékenységi körben ellátja az EU rendeletben és az Infotv-ben, továbbá a személyes adatok védelmével és a közérdekű adatok nyilvánosságával összefüggő feladatok irányításáról és felügyeletéről, valamint az ezekhez kapcsolódó egyes tevékenységek eljárási rendjéről szóló 2/2019. (I.24.) HM utasításban (a továbbiakban: Utasítás) részére meghatározott feladatokat.

Az adatvédelmi tisztviselőt távolléte esetén a Jogi és Igazgatási Alosztály vezetője helyettesíti.

Az Utasítás vonatkozó rendelkezése értelmében nem láthat el adatvédelmi tisztviselői feladatot a honvédelmi szervezet vezetője, helyettesei, személyügyi szerv vezetője, a pénzügyi vezető, az informatikai vezető és a rendszergazda. A felsorolt beosztásokon túl azon beosztást ellátó sem lehet adatvédelmi tisztviselő, aki adatkezelési művelet végrehajtásáért felelős szerv vezetője.

Az adatvédelmi tisztviselő ezen feladatai ellátása során közvetlenül a parancsnoknak van alárendelve, tevékenységéről részére számol be, javaslatait számára teszi meg. Az adatvédelmi tisztviselő feladatai a munkaköri leírásában kerülnek rögzítésre.

Az adatvédelmi tisztviselő kijelölésének feltételei, alárendeltsége, feladatai, a rá vonatkozó összeférhetetlenségi szabályok, valamint a tevékenysége ellátását biztosító források tekintetében az Utasításban foglaltak az irányadók.

Az adatvédelmi tisztviselő nevét, elérhetőségeit meg kell küldeni a Honvédelmi Minisztérium (a továbbiakban: HM) Jogi Főosztály Adatvédelmi Osztály (a továbbiakban: HM JF AO), mint szakmai szerv és a Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: NAIH) részére.

Az adatvédelmi tisztviselő neve, elérhetőségei a szervezet honlapján közzétételre kerülnek, továbbá ezen adatai bejelentésre kerültek a NAIH részére.

Az adatvédelmi tisztviselő az alábbi elektronikus nyilvántartásokat vezeti:
a) adatvagyon leltár,
b) adatkezelési tevékenységek nyilvántartása, adatkezelői nyilvántartás összesítése,
c) adatfeldolgozói tevékenységek nyilvántartása, adatfeldolgozói nyilvántartás (ha van ilyen tevékenység),
d) adatvédelmi incidensek nyilvántartása (ha történik ilyen),
e) az előzetes kockázatelemzésekről, hatásvizsgálatokról szóló nyilvántartás,
f) adatközlési, adattovábbítási nyilvántartás (ha van ilyen tevékenység),
g) az érintett jogainak érvényesítésével kapcsolatos nyilvántartás (ha volt ilyen beadvány),
h) a beérkezett közérdekű adatigénylésekről (ha volt ilyen).

Az adatvédelmi tisztviselő papír és elektronikus formában vezeti az adatkezelési tevékenységek nyilvántartását és az adatkezelői nyilvántartást. A nyilvántartások folyamatosan aktualizálásra kerülnek.

Az adatvédelmi tisztviselő minden év november 15-ig ellenőrzési tervet készít, melyet az MH KIBP parancsnoka hagy jóvá. Az adatvédelmi tisztviselő ellenőrzéseit az éves tervnek

megfelelően köteles végrehajtani, azok eredményéről, – amennyiben elöljárói intézkedésre okot adó körülményt észlel – jelentést készít az MH KIBP, érintettség esetén az MH KIMK parancsnoka részére.

Az adatvédelmi tisztviselő évente legalább egyszer oktatást tart a szervezet tagjainak. Az oktatást követően a személyi állomány köteles vizsgát tenni, lehetőség szerint az erre kialakított elektronikus felületen keresztül.

Az adatvédelmi tisztviselőt minden személyes adatra vonatkozó egyedi megkeresésről haladéktalanul értesíteni kell.

A kérelemre történő személyes adat kiadása előtt az adatvédelmi tisztviselőt értesíteni kell, vele egyeztetni szükséges.

Az adatkezelő és az adatfeldolgozó személyi állományának tagjait időbeli korlátozás nélkül titoktartási kötelezettség terheli, függetlenül attól, hogy az adatot közvetlenül az érintettől, illetve közvetett módon az adatkezelő dokumentációiból, vagy bármely más módon ismerték meg.

Az adatkezelő munkavállalói titoktartási nyilatkozatot írnak alá.

7. Az adatvédelmi kapcsolattartó és feladatai

Az MH KIMK parancsnoka személyi állományából - adatvédelmi tisztviselőnek nem minősülő - adatvédelmi kapcsolattartót, annak távolléte idejére helyettest jelöl ki és erről az MH KIBP parancsnokát értesíti.

Az adatvédelmi kapcsolattartó az MH KIMK szervezeti egységeinél figyelemmel kíséri az adatkezeléssel foglalkozó személyek tevékenységét, szükség esetén felhívja a figyelmet a vonatkozó szabályok betartására, ismételt vagy súlyos adatvédelmi szabálytalanság észlelése estén haladéktalanul értesíti az adatvédelmi tisztviselőt.

Adattovábbítás kezdeményezése esetén haladéktalanul, de legkésőbb az adattovábbításra irányuló megkeresés beérkezésétől számított 2 munkanapon belül szóban és írásban is értesíti az adatvédelmi tisztviselőt, akivel egyeztet az adattovábbításról. Az adatvédelmi tisztviselő szintén haladéktalanul, de legkésőbb 2 munkanapon belül értesíti a HM JF AO -t és a Honvéd Vezérkar (a továbbiakban: HVK) adatvédelmi tisztviselőjét az adattovábbításról.

Az előző pont szerinti írásbeli értesítésnek legalább az alábbi adattartalommal kell rendelkeznie:

a) az adattovábbítás jogalapja és címzettje, és

b) a személyes adatok köre.

A személyes és közérdekű adatokkal kapcsolatos megkeresésekről haladéktalanul tájékoztatják az MH KIBP adatvédelmi tisztviselőjét.

Az adatvédelmi kapcsolattartó a fentieken túl ellátja az alábbi feladatokat:

a) összegyűjti és átadja az adatvédelmi tisztviselőnek az adatkezelés dokumentálásához szükséges információkat, iratokat,

b) a tudomására jutott, az érintetti jogokkal kapcsolatos kérelmek tekintetében összegyűjti a releváns információkat, és az adatvédelmi tisztviselő rendelkezésére bocsátja,

c) haladéktalanul tájékoztatja az adatvédelmi tisztviselőt az önálló szervezeti egységnél bekövetkezett, tudomására jutott adatvédelmi incidensről,

d) összegyűjti a releváns információkat az önálló szervezeti egység adatkezelését érintő kockázatelemzés elkészítéséhez, és

e) az adatvédelmi tisztviselő javaslata esetén részt vesz az önálló szervezeti egységet érintő hatásvizsgálat lefolytatásában.

Az adatvédelmi feladatban, incidensben érintett ügyintézők, vezetők, kötelesek az adatvédelmi kapcsolattartó részére az adatvédelmi tisztviselő által meghatározott adatokat, információkat átadni.

Az adatvédelmi kapcsolattartót a megismert adatokkal, információkkal kapcsolatban titoktartási kötelezettség terheli.

8. Az adatvédelem alapelvei

Adatkezelés az EU rendelet hatálya alá tartozó adatkezelések esetében az 5. cikkében, az Infotv. hatálya alá tartozó adatkezelések esetében pedig az Infotv. 4 §-ában meghatározott alapelvek fennállása esetén végezhető.

9. Az adatkezelések feltételei

Személyes adatot kezelni csak úgy lehet, ha annak célja vagy céljai egyértelműen, közérthetően meghatározásra kerültek. Az adatkezelés céljának jogszerűnek, továbbá már az adatok gyűjtésének időpontjában megfogalmazottnak kell lennie.

Minden adatkezelés megkezdése előtt meg kell vizsgálni, hogy a meghatározott cél adatkezelés nélkül megvalósulhat-e.

A kezelt személyes adatoknak alkalmasnak és szükségesnek kell lenniük a meghatározott cél elérésére.

Kizárólag annyi adatot lehet kezelni, amennyi a cél eléréséhez feltétlenül szükséges és a cél elérésére alkalmas.

A személyes adatokat a lehető legrövidebb ideig lehet tárolni, ennek érdekében törlési vagy rendszeres felülvizsgálati határidőket kell megállapítani.

A személyes adatokat az egyes adatkezelések esetében a cél megvalósulásáig, illetve meghatározott ideig lehet megőrizni.

Adatkezelés az EU rendelet hatálya alá tartozó adatkezelések esetében a 6. cikk (1) bekezdésében, az Infotv. hatálya alá tartozó adatkezelések esetében pedig az Infotv. 5. §-ban meghatározott jogalapok valamelyikének fennállása esetén végezhető.

Az EU rendelet 6. cikk (1) bekezdés f) pontjában meghatározott jogalap alkalmazása esetén érdekmérlegelési teszt elkészítése szükséges, melynek lefolytatásába az adatvédelmi tisztviselőt be kell vonni.

Az érdekmérlegelési teszt írásbeli dokumentáció arról, hogy az adatkezelés az adatkezelő jogos érdeke vagy érdekei érvényesítéséhez szükségesek és ezen érdek vagy érdekek elsőbbséget élveznek az érintett érdekeivel, jogaival szemben. Ezentúl tartalmazza az adatkezelés végrehajtásának módját, továbbá azt, hogy az adatkezelő milyen érintetti érdekeket védő garanciákat épít be az adatkezelési folyamatba.

Az érdekmérlegelési teszt elkészítése az adatkezelési művelet végrehajtásáért felelős szervezeti egység vezetőjének felelősségi körébe tartozik. Az érintettet az érdekmérlegelés

tényéről és a teszt eredményéről tájékoztatni kell. Az érdekmérlegeléssel összefüggő tevékenységet dokumentálni kell, és az ezzel kapcsolatos iratokat az adatvédelmi tisztviselő részére át kell adni.

Az érdekmérlegelési teszt eljárási rendje:
a) az adatkezelő jogos érdekének beazonosítása és megfogalmazása,
b) az érintett érdekeinek, jogainak és szabadságainak beazonosítása és megfogalmazása,
c) a mérlegelés elvégzése, melynek során különösen azt kell vizsgálni, hogy miért szükséges az adatkezelés, megvalósul-e a célhoz kötöttség, milyen adatkezeléseket hajt végre az adatkezelő, érvényesülnek– e az adatkezelések elvei és az érintetti jogok,
d) annak meghatározása, hogy miért korlátozza arányosan a katonai szervezet jogos érdeke az érintett személyek jogait és szabadságait.

10. Az érintett jogai és érvényesítésük

Az érintett által megküldött, a jogai gyakorlásával kapcsolatos levelet, amennyiben azt nem az adatvédelmi tisztviselőnek címezték, részére haladéktalanul továbbítani szükséges. Amennyiben a levél tartalmi beazonosítása kétséges, úgy azzal kapcsolatban ki kell kérni az adatvédelmi tisztviselő véleményét.

Az érintettet megillető jogokkal kapcsolatos igény érvényesítésének teljesítésére kizárólag az érintettek adatainak védelmét szolgáló adatbiztonsági követelményeket szem előtt tartva, csak a kérelmező megfelelő azonosítása esetén van lehetőség.

Az érintett a személyes adatainak kezeléséről tájékoztatást kérhet az adatkezelőtől.
Az adatkezelő
a) az EU rendelet hatálya alá tartozó adatkezelés esetén indokolatlan késedelem nélkül, de legfeljebb a kérelem beérkezéstől számított 1 hónapon belül tájékoztatja az érintettet. Szükség esetén – figyelemmel a kérelem összetettségére és a kérelmek számára – a határidő további 2 hónappal meghosszabbítható. A határidő meghosszabbításáról az adatkezelő a késedelem okainak megjelölésével a kérelem kézhezvételétől számított egy hónapon belül tájékoztatja az érintettet.

b) az Infotv. hatálya alá tartozó adatkezelése esetén az adatkezelő a legrövidebb idő alatt, de legfeljebb 25 napon belül tájékoztatja az érintettet. Határidő hosszabbítására nincs lehetőség.

Megalapozatlan vagy egy éven belül azonos adatkörre vonatkozó kérelem esetén az adatkezelő a kérelem teljesítése vonatkozásában a felmerült költségek megtérítését követelheti vagy – kizárólag a EU rendelet hatálya alá tartozó adatkezelés esetén – a kérelmet elutasíthatja. A többlet költségtérítés alapjául szolgáló díjak vonatkozásában az Utasításban foglaltak irányadók.

A megalapozatlanságra, a túlzó jellegre alapított megtagadás, illetve a többlet költségfelszámolás okának bizonyítása az adatkezelőt terheli, ennek érdekében, az eljárást megfelelően dokumentálni szükséges.

Az EU rendelet hatálya alá tartozó adatkezelések esetén,
a) amennyiben az adatkezelő az érintettől szerzi be az adatokat, az EU rendelet 13. cikke szerinti,

b) az a) pontban foglaltaktól eltérő adatszerzés során az EU rendelet 14. cikke szerinti tájékoztatót kell az érintett részére rendelkezésre bocsátani.

Az Infotv. hatálya alá tartozó adatkezelések esetében az érintetteket az Infotv. 16. §-ában meghatározottak szerint kell tájékoztatni.

Az adatkezelő az EU rendelet hatálya alá tartozó adatkezelések tekintetében az EU rendelet 13. vagy 14. cikke szerinti tájékoztatón túl – az EU rendeletben meghatározott feltételek fennállása esetén – biztosítja az érintettek
a) hozzáférési jogát,
b) helyesbítéshez való jogát,
c) törléshez való jogát,
d) adatkezelés korlátozásához való jogát,
e) adathordozhatósághoz való jogát,
f) tiltakozáshoz való jogát,
g) az EU rendelet 22. cikke szerinti jogát automatizált döntéshozatal, profilalkotás alkalmazása esetén.

Az adatkezelő az Infotv. hatálya alá tartozó adatkezelések esetében – az Infotv.-ben meghatározott feltételek fennállása esetén – biztosítja az érintettek
a) előzetes tájékozódáshoz való jogát,
b) hozzáféréshez való jogát,
b) helyesbítéshez való jogát,
c) törléshez való jogát és
d) az adatkezelés korlátozásához való jogát.

Az érintett személyes adatai kezelésének megsértésével kapcsolatban indult bármely eljárásról az adatvédelmi kapcsolattartó értesíti az adatvédelmi tisztviselőt.

Az érintett személyes adatai kezelésével kapcsolatos vélt jogsérelem esetén az adatvédelmi tisztviselőhöz, az illetékes törvényszékhez fordulhat, vagy vizsgálatot kezdeményezhet a NAIH-nál.

11. Adatvédelmi incidens kezelése, jelentése

Az MH KIBP és az MH KIMK, az adatvédelmi incidensek megelőzése és felderítése érdekében technikai és szervezési intézkedéseket vezet be és ezen intézkedések betartását rendszeresen ellenőrzi:
a) jelen intézkedésben előírja az adatvédelem szabályozási rendszerét, szervezetét,
b) kijelöli az adatvédelmi tisztviselőt,
c) a személyi állományt folyamatosan tájékoztatja az adatvédelmi előírásokról, részükre évente legalább egy alkalommal oktatást tart, illetve vizsgáztatást hajt végre az adatvédelmi tisztviselő útján,
d) informatikai eszközök segítségével megakadályozza a személyes adatok jogellenes kezelését, vagy az azokhoz történő jogellenes hozzáférést,
e) a személyi állomány a személyes adatokat kizárólag előre meghatározott jogosultságok alapján kezelheti,
f) egyéb adatbiztonsági intézkedéseket vezet be.

Az MH KIBP, mint adatkezelő köteles ennek tényét regisztrálni a NAIH honlapján. Adatvédelmi incidens gyanúja esetén a közvetlen elöljáró vagy munkahelyi vezető útján az adatvédelmi tisztviselőt haladéktalanul értesíteni kell. Az adatvédelmi incidenssel kapcsolatos releváns információkat, így különösen

- hogy az adat biztonsága sérült-e,
- az incidenssel érintettek köre és száma,
- az érintett adatok kategóriája és száma - ha meghatározható -,
- a már megtett vagy tervezett adatbiztonsági intézkedések,
- az eset körülményei;
- milyen mértékben érinti az érintett jogait, szabadságait

az adatvédelmi tisztviselő részére át kell adni, aki haladéktalanul értesíti a HM JF AO-t valamint a Honvéd Vezérkar adatvédelmi tisztviselőjét, továbbá, ezzel egyidejűleg az adatvédelmi incidenst bejelenti a NAIH incidens bejelentő rendszerébe.

Az adatvédelmi incidens bekövetkezését követően a parancsnok, akadályoztatása esetén a parancsnok-helyettes, haladéktalanul intézkedik incidens-kezelési munkacsoport (a továbbiakban: IMCS) felállítására, tagjait az adatvédelmi incidens jellegének megfelelően az adott témakör szakértői köréből kijelöli.

Az IMCS alapvetően

- az adatvédelmi tisztviselőből,
- az incidenssel érintett adatkezelést végző osztály vagy alosztály vezetőjéből,
- elektronikus adatkezelés esetén az MH KIBP, az MH KIMK parancsnoka vagy az MH KIMK Kiberbiztonsági és Védelmi Osztály osztályvezetője által kijelölt informatikus vagy megfelelő ismeretekkel rendelkező szakemberből,
- olyan adatkezelés esetén, amely során minősített adatok és rendszerek érintettek, a biztonsági vezetőből áll.

Az IMCS összehívására a parancsnok, a parancsnok helyettese, valamint az adatvédelmi tisztviselő jogosult. Az adatvédelmi incidens bekövetkezését követően a felállított IMCS-t 24 órán belül össze kell hívni.

Az IMCS megvizsgálja, hogy

a) az adat biztonságának sérülése érinti-e a személyes adatok biztonságát,
b) kockázatos-e az adat biztonságának sérülése az érintettek jogaira és szabadságaira nézve, különös tekintettel az adatvédelmi incidenssel érintett adatok típusára, mennyiségére,
c) milyen intézkedések tehetők a kockázatok csökkentésére,
d) szükséges-e az adatvédelmi incidens bejelentése a NAIH felé, és
e) szükséges-e az adat sérülésével érintettek értesítése.

Az IMCS a rendelkezésére álló adatok és az adatkezelés helyszínén végzett elemzés alapján dönt

a) az esemény adatvédelmi incidensnek történő nyilvánításáról, vagy
b) az incidensnek nyilvánítás mellőzéséről.

Amennyiben az IMCS az eseményt adatvédelmi incidensként értékelte, dönt arról, hogy az milyen kockázatú, 24 órán belül értesíti erről a HM JF AO-t, valamint tájékoztatja a HVK adatvédelmi tisztviselőjét.

Az adatvédelmi incidens kockázata

a) alacsony, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve,

b) közepes, ha az adatvédelmi incidens valószínűsíthetően kockázattal jár az érintettek jogaira és a negatív következményeket nem lehet intézkedésekkel hatékonyan elhárítani,
c) magas, ha az adatvédelmi incidens az érintettekre jelentős vagy akár visszafordíthatatlan következményekkel, vagy komoly nehézségekkel járna vagy járhatna.

Az IMCS az adatvédelmi incidens kockázata értékelésénél megvizsgálja
a) az Adatkezelési Környezetet (AK), melynek során feltérképezi a sérült adatok fajtáit, az adatkezelés valamennyi körülményét,
b) az Azonosíthatóság Mértékét (AM), amely annak meghatározását jelenti, hogy az incidenssel érintett adatokból mennyire könnyen lehet az érintettek azonosítását elvégezni,
c) a Sérülés Körülményeit (SK), a sérült adatok biztonságának csökkenését, a rosszindulatú támadásra és szándékosságra utaló jeleket.

Ha adatvédelmi incidens történt és az IMCS döntése alapján az valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve, az adatvédelmi incidenst az incidens nyilvántartásban szükséges rögzíteni.

Amennyiben az IMCS megállapítja, hogy az adatvédelmi incidens közepes vagy magas kockázatú, az IMCS javaslatot tesz az adatkezelő részére az adatvédelmi incidens következményeinek mérséklését célzó intézkedésekre, az adatvédelmi tisztviselő értesíti a HM JF AO-t, valamint 72 órán belül az incidensbejelentő rendszeren bejelenti a NAIH felé.

Amennyiben az IMCS döntése alapján az adatvédelmi incidens valószínűsíthetően magas kockázattal jár az érintettek jogaira és szabadságaira nézve, a lehető leghamarabb értesíteni kell az érintetteket is az incidensről, annak érdekében, hogy a megfelelő intézkedéseket meg tudják tenni.

A tájékoztatás mellőzhető, amennyiben az adatkezelő a személyes adatok védelme érdekében megfelelő technikai intézkedéseket tett, vagy hatékony intézkedések eredményeként a magas kockázat következményei valószínűsíthetően nem következnek be.

Amennyiben a közvetlen tájékoztatás lehetetlen vagy aránytalan erőfeszítéssel járna, a tájékoztatást egyéb módon kell megtenni, ilyen lehet a szervezet honlapján közzétett nyilvános tájékoztató.

Az IMCS a tevékenységéről köteles teljes körű dokumentációt vezetni, melyben részletesen rögzítik a döntések alapjait, körülményeit.

A személyi állomány kötelezettségei az adatvédelmi incidenssel kapcsolatban:
a) bármilyen csekély jelentőségűnek vélt adatvédelmi incidenst köteles az észlelést követően azonnal, késedelem nélkül jelenteni a közvetlen elöljárónak vagy munkahelyi vezetőnek,
b) az adatvédelmi incidens körülményeit feljegyezni és azt a közvetlen elöljárónak, vagy munkahelyi vezetőnek jelenteni, így különösen: az észlelés pontos időpontját, a bekövetkezés pontos időpontját (amennyiben az megállapítható), az érintett személyes adatok körét, és az általa észlelt egyéb körülményeket.

12. Adatvédelmi hatásvizsgálat

Az adatkezelést megelőzően az érintett adatkezelési művelet végrehajtásáért felelős szervezeti egység a tervezett adatkezelés kockázatainak megállapítása érdekében előzetes kockázatértékelést végez, amelynek eredményéről tájékoztatja az adatvédelmi tisztviselőt. A hatásvizsgálat célja az adatkezelés szükségességének és arányosságának, jellegének feltárása, vizsgálata, valamint a kockázatok kezelésének elősegítése.

Az adatvédelmi tisztviselő szakmai tanácsadást nyújt az adatvédelmi hatásvizsgálat elvégzéséhez, valamint nyomon követi az elkészítését.

Az adatkezelést megelőzően hatásvizsgálatot kell végezni,
a) ha az adatkezelés valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve,
b) ha új technológia kerül alkalmazásra,
c) a NAIH által közzétett esetekben.

Az EU rendelet 75. preambulum bekezdése szerint magas kockázatú az adatkezelés, ha:
a) nagyszámú érintettre, nagy mennyiségű adatra vonatkozik,
b) különleges adatokat vagy kiszolgáltatott személyek adatait érinti,
c) profilalkotás történik,
d) az érintettek nem rendelkezhetnek személyes adataik felett, nem gyakorolhatják jogaikat, szabadságaikat,
e) pénzügyi veszteség, fizikai, vagyoni, nem vagyoni kár kockázata áll fenn,
f) jó hírnév sérelmének, bizalmasság megsértésének, személyazonossággal való visszaélés veszélyének lehetősége áll fenn.

Amennyiben az adatvédelmi tisztviselő megítélése szerint a tervezett adatkezelés kockázatos, úgy munkacsoport létrehozására tesz javaslatot a parancsnok részére. A munkacsoport feladata az adatkezelés kockázatainak vizsgálata és értékelése.

A hatásvizsgálat elvégzését a munkacsoport az adatkezelés minden elemének figyelembevételével, a szakmai szerv által rendelkezésre bocsátott hatásvizsgálati módszer alkalmazásával végzi el, és ennek alapján hozza meg döntését. A hatásvizsgálat lezárásáig az adatkezelést nem lehet megkezdeni.

A munkacsoport vezetője az adatkezelési művelet végrehajtásáért felelős szervezeti egység vezetője. A munkacsoport munkájában való részvételre a vezető a szervezeti egységéből maga helyett – akadályoztatása esetén – más személyt is kijelölhet.

A munkacsoport tagjai:
a) az adatkezelési művelet végrehajtásáért felelős szervezeti egység vezetője,
b) az adatvédelmi tisztviselő, a munkacsoport vezetője által az állományából kijelölt személy,
d) elektronikus adatkezelés esetén megfelelő szakmai ismeretekkel rendelkező személy,
e) olyan adatkezelés esetén, amely során minősített adatok és rendszerek érintettek, a biztonsági vezető.

Amennyiben a hatásvizsgálat magas kockázatot állapít meg, az MH KIBP előzetes konzultációt kezdeményez a NAIH-hal a HM JF AO-al történt egyeztetést követően.

Nem szükséges hatásvizsgálatot végezni, ha

a) az adatkezelés valószínűsíthetően nem jár magas kockázattal,
b) egymáshoz hasonló típusú adatkezelési műveletek esetében, amelyek egymáshoz hasonló kockázatokat jelentenek. Ebben az esetben egyetlen hatásvizsgálat is elegendő (EU rendelet, 35. cikk (1) bekezdés),
c) az EU rendelet 6. cikk (1) bekezdésének c) vagy e) pontja szerinti adatkezelés (az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez vagy az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges) jogalapját uniós vagy az adatkezelőre alkalmazandó tagállami jog írja elő, és e jog a szóban forgó konkrét adatkezelési műveletet vagy műveleteket is szabályozza, valamint e jogalap elfogadása során egy általános hatásvizsgálat részeként már végeztek adatvédelmi hatásvizsgálatot (EU rendelet 35. cikk (10) bekezdés),
d) a NAIH azon listáján szerepel, amely szerint az adott kezelés tekintetében nem kötelező hatásvizsgálatot végezni.

13. Az adatbiztonság

Az adatbiztonsági és kockázatkezelési előírások részletes meghatározását a honvédelmi tárca információbiztonság politikájáról szóló 94/2009. (XI. 27.) HM utasítás vonatkozó rendelkezései, valamint a honvédelmi tárca általános elektronikus információbiztonsági követelményeinek meghatározásáról és a védelmi rendszabályok pontosításáról szóló 3/2012. (I. 13.) HM utasítás tartalmazza.

Az iratkezelésre a Magyar Honvédség Egységes Iratkezelési Szabályzatának kiadásáról, valamint a Honvédelmi Minisztérium és a Magyar Honvédség Titokvédelmi és Ügyviteli Szabályzata kiadásáról szóló 11/1996. (HK 7.) HM utasításban foglaltak az irányadók.

Az adatkezelő adatkezelései papír alapon és elektronikus formában történhetnek.

Az adatkezelő a személy azonosítására alkalmas jellegétől megfosztott, újonnan képzett adatokat statisztikák, belső kimutatások készítésére felhasználhatja. Az adatkezelő anonimizálást alkalmaz minden olyan esetben, amikor anonim adatok is elégségesek, valamint ahol szerződés vagy jogszabály írja elő a statisztikai adatok szolgáltatását.

Az adatok megőrzési ideje adatkezelésenként kerül meghatározásra.

Az MH KIBP a megőrzési idő lejártával az elektronikus adathordozóról fizikailag törli a személyes adatokat. Az adathordozók selejtezésekor, esetleges központi készletbe rendeléskor, valamint a katonai szervezetek közötti átadás/átvétel esetén ugyanígy jár el.

Amennyiben az adathordozó papíralapú, vagy az elektronikus adathordozó nem törölhető fizikailag, akkor fizikailag – a helyreállíthatóság kizárásával – meg kell semmisíteni azokat. A megsemmisítési eljárást úgy kell kialakítani, hogy a művelet után ne lehessen visszaállítani az adatokat.

Az MH KIBP a papíralapú adathordozókon tárolt adatok megsemmisítését a vonatkozó szabályok szerint végzi.

Az adat törlését minden esetben az adatkezelési műveletet végző szervezeti egység vezetője kezdeményezi. A törlésről, megsemmisítésről jegyzőkönyvet kell készíteni. A jegyzőkönyv tartalmazza különösen az adatkezelés célját, annak kezdő és befejező időpontját,

a törlendő, megsemmisítendő adatok fajtáját, a törlés időpontját, módját, valamint a törlés, megsemmisítés elrendelőjének személyét.

14. Adatkezelést végrehajtó ügyintézők

Az adatkezeléssel foglalkozó ügyintézők közül azok, akik KGIR hozzáféréssel rendelkeznek, kizárólag a jogosultságaiknak megfelelő adatkezelési tevékenységet végezhetnek.

Az ügyintéző gondoskodik arról, hogy jogosulatlan személyek ne tekinthessenek be személyes vagy különleges adatokba, továbbá arról, hogy a személyes vagy különleges adat tárolása, elhelyezése úgy kerüljön kialakításra, hogy az jogosulatlan személy részére ne legyen hozzáférhető, megismerhető, megváltoztatható, megsemmisíthető.

Az ügyintéző a helyiséget, ahol adatkezelés történik, a nap folyamán csak úgy hagyhatja el, hogy az adathordozókat elzárja, a számítógépből kijelentkezik, vagy az irodát bezárja. A munkavégzés befejeztével az adathordozót el kell zárni.

15. Az adatfeldolgozás

Az MH KIBP adatkezelési tevékenységeihez adatfeldolgozót vehet igénybe.

Az adatfeldolgozásról szerződésben kell rendelkezni, melynek tartalmánál figyelembe kell venni a hatályos adatvédelmi követelmények érvényesülését, különösen az adatfeldolgozás műveleteinek meghatározására, az adatkezelés garanciáira, az adatkezeléssel kapcsolatos tájékoztatási kötelezettségekre, az MH KIBP ellenőrzési jogára tekintettel.

Az adatfeldolgozó tevékenységét rögzített követelményrendszer betartása mellett az MH KIBP utasításai alapján látja el.

Az adatfeldolgozásra vonatkozó szerződés előkészítésébe az adatvédelmi tisztviselőt be kell vonni.

Az adatfeldolgozásra vonatkozó szerződésnek különösen a következőket kell tartalmaznia:

a) az adatkezelő és az adatfeldolgozó személyét, elérhetőségét, ha az adatfeldolgozó rendelkezik adatvédelmi tisztviselővel, annak elérhetőségét,

b) adatkezelés célját,

c) az adatfeldolgozás jellegét, célját, időtartamát,

d) az adatfeldolgozással érintett adatalanyok kategóriáit, a személyes adatok típusát, mennyiségét,

e) az adatkezelő és adatfeldolgozó jogainak és kötelezettségeinek meghatározását, különösen annak rögzítését, hogy az adatfeldolgozó az adatkezelő kifejezett írásos utasításai alapján végezhet adatkezelési műveleteket, továbbá az esetlegesen bekövetkező adatvédelmi incidensek esetén követendő szabályok meghatározását,

f) az elvégzett technikai műveletek megnevezését, módját,

g) a feldolgozott személyes adatok további sorsát,

h) annak rögzítését, hogy az adatfeldolgozó további adatfeldolgozót vehet-e igénybe,

i) az adatkezelőt és az adatfeldolgozót terhelő technikai és szervezési intézkedések meghatározását, ezek igazolását az adatfeldolgozó részéről,

j) az adatfeldolgozó azon alkalmazottai titoktartására vonatkozó rendelkezéseket, akik az adatfeldolgozásban részt vesznek,

k) annak szabályozását, hogy az adatfeldolgozó milyen módon, eljárási rendet követve

nyújt segítséget az érintettek jogait érintő kérelmek megválaszolásában,
l) az adatkezelő ellenőrzési jogkörének biztosítását,
m) az adatkezelő utasításadási rendjének meghatározását, beleértve az adatfeldolgozó azon kötelezettségét, hogy tájékoztassa az adatkezelőt, ha az adatkezelő által adott utasítás az EU rendeletbe vagy egyéb vonatkozó jogszabályba ütközik.

16. Adatközlés, adattovábbítás

Az érintettek személyes adatainak közlésére, továbbítására kizárólag jelen szabályzatban meghatározottak szerint és a feltételek megvalósulása esetén kerül sor.

Harmadik fél részére adat csak akkor közölhető, továbbítható, ha
a) az érintett ehhez az adatkezelés során előzetesen hozzájárulását adta és ha az adatkezelés feltételei minden egyes adatra nézve teljesülnek,
b) a törvény vagy helyi önkormányzati rendelet az adatközlést, adattovábbítást megengedi és az adatkezelés feltételei minden egyes személyes adatra nézve teljesülnek,
c) az adatkezelőre vonatkozó jogi kötelezettség teljesítése céljából szükséges,
d) az adatkezelő vagy harmadik személy jogos érdekének érvényesítése céljából szükséges, és ezen érdek érvényesítése a személyes adatok védelméhez fűződő jog korlátozásával arányban áll,
e) a nemzetbiztonság, a honvédelem és a közbiztonság védelme, a bűncselekmények üldözése céljából az arra hatáskörrel rendelkező nemzetbiztonsági szerveknek, nyomozó hatóságoknak, bíróságoknak, valamint egyéb bírósági és nyomozó szervek jogszerű megkeresése esetén átadhatók az adattovábbítási kérésben megjelölt adatok tekintetében.

Az adatvédelmi tisztviselő szakmai véleményét ki kell kérni az adatközlést, adattovábbítást megelőzően.

17. Elektronikus közzététel

Az MH KIBP az Infotv. 24/A. alpontjában foglaltak alapján csatlakozni köteles az egységes közadatkereső rendszerhez, melybe feltölti az Infotv. 37/B. és 37/C. §-aiban meghatározott adatokat.

Az egységes közadatkereső rendszerhez csatlakozáskor kapcsolattartónak az MH KIBP adatvédelmi tisztviselője minősül.

Az Utasítás 9. mellékletében szereplő általános közzétételi listában szereplő adatokat az változás esetén az általános közzétételi lista szerint meghatározott gyakorisággal frissíteni kell. A frissített adatokat az adatvédelmi tisztviselő a HM JF AO részére megküldi.

18. Közérdekű adatigénylés teljesítésének rendje

Az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szervnek vagy személynek lehetővé kell tennie, hogy a kezelésében lévő közérdekű adatot és közérdekből nyilvános adatot erre irányuló igény alapján bárki megismerhesse, az alábbi kivételekkel.

A közérdekű és közérdekből nyilvános adatok megismeréséhez való jogot törvény

a) honvédelmi érdekből,
b) nemzetbiztonsági érdekből,
c) bűncselekmények üldözése vagy megelőzése érdekében,
d) környezet- vagy természetvédelmi érdekből,
e) központi pénzügyi vagy devizapolitikai érdekből,
f) külügyi kapcsolatokra, nemzetközi szervezetekkel való kapcsolatokra tekintettel, bírósági vagy közigazgatási hatósági eljárásra tekintettel,
g) a szellemi tulajdonhoz fűződő jogra tekintettel
korlátozhatja.

Az MH KIBP-re érkező közérdekű adatigénylések esetén az MH KIBP adatvédelmi tisztviselője az adatigénylést, a választervezetet és az 1. számú mellékletben meghatározott elszámoló ívet a válasz szakmai kidolgozása, annak összeállítása és a felmerülő dologi kiadások becslése céljából haladéktalanul megküldi a HM JF AO- ra és a HM kommunikációért felelős szervezet részére.

A jóváhagyott választervezetet az MH KIBP az igény beérkezésétől számított legfeljebb 15 napon belül megküldi az adatigénylő részére.

19. Közérdekű adatigénylés teljesítéséért megállapítható költségtérítés

A válaszadásra kötelezett az adatigénylés teljesítéséért az Infotv. 29. § (3) és (4) bekezdéseiben, valamint a közérdekű adat iránti igény teljesítéséért megállapítható költségtérítés mértékéről szóló 301/2016. (IX. 30.) Korm. rendeletben (a továbbiakban: Korm. rendelet) meghatározott feltételek fennállása esetén és mértékig költségtérítést állapíthat meg.

A választervezetet kidolgozó előzetesen megbecsüli a felmerülő dologi kiadások összegét (az adathordozó/másolat készítésének, illetve kézbesítés költsége), ezt követően az elszámoló ívet haladéktalanul megküldi a válaszadásra kötelezett részére.

Költségtérítés esetén a válaszadásra kötelezett tájékoztatja az adatigénylőt a költségtérítésről. Az igénylőnek ezt követően 30 napja van, hogy eldöntse, fenntartja-e az adatigénylést. Amennyiben igen, erről nyilatkoznia kell és az adatkezelő által megállapított, a nyilatkozat megtételétől számított legalább 15 napos határidő alatt az összeget be kell fizetnie. A megfizetést követő 15 napon belül az adatokat számára ki kell adni.

Ha az adatigénylés teljesíthető másolatkészítést nem igénylő módon is, az adatigénylőt erről is tájékoztatni kell.

Költségtérítés esetén a tájékoztatáshoz csatolni kell a 2. számú mellékletben meghatározott formanyomtatványt, és az adatigénylőt fel kell kérni arra, hogy a tájékoztatást követő igénylésének fenntartása esetén azt megfelelően kitöltve küldje vissza.

A költségtérítéssel kapcsolatos számla kibocsátása a MH Szentendrei Helyőrség Támogató Parancsnokság Gazdálkodás Támogató és Pénzügyi Ellátó Referatúra feladata. A költség adatigénylő általi megfizetésének tényét a pénzügyi referatúra haladéktalanul jelzi a válaszadásra kötelezettnek.

Az alcímben nem szabályozott kérdésekben a Korm. rendeletben meghatározottak szerint kell eljárni.

20. Záró rendelkezések

Jelen intézkedés az aláírás napján lép hatályba, melyet a teljes állomány részére ki kell hirdetni.

Mellékletek:

1. sz. melléklet: ELSZÁMOLÓ ÍV a közérdekű adatigényléshez kapcsolódó költségtérítéshez (.docx)

2. sz. melléklet: Az adatigénylő költségtérítés megfizetésének teljesítéséhez szükséges személyes adatai (.docx)

Budapest, „időbélyeg szerint”

Pozderka Gábor ezredes
parancsnok

A hatályos jogszabályokkal összhangban áll.

Budapest, „az EIR-ben rögzített dátummal”

Szathmáry Katalin honvédelmi alkalmazott s.k.
Jogi és Igazgatási Alosztály
alosztályvezető

Készült: 1 példányban
Egy példány: 18 lap
Ügyintéző (tel.): dr. Molnár Erzsébet szds. (252-16)
Kapják: 1.sz. példány: Irattár
2.sz. példány: MH KIMK

MAGYAR HONVÉDSÉG
KIBERMŰVELETI PARANCSNOKSÁG

E- ALÁÍRÓÍV

Aláírta: Pozderka Gábor
Időpont: 2023.04.26 16:07:54 CEST