MAGYAR HONVÉDSÉG BOCSKAI ISTVÁN
11. PÁNCÉLOZOTT HAJDÚDANDÁR
ADATVÉDELMI ÉS ADATBIZTONSÁGI SZABÁLYZATA

Jelen Szabályzatot a 473/2024. MH BI 11. pctt. dd. PK. intézkedés léptette hatályba.

Tartalomjegyzék

1. A Szabályzat hatálya, célja

1. A Szabályzat személyi hatálya kiterjed a Magyar Honvédség Bocskai István 11. Páncélozott Hajdúdandár (a továbbiakban: Dandár) teljes személyi állományára.

Az intézkedés célja, hogy:

a) Meghatározza azokat az intézkedéseket, amelyek biztosítják a Dandár által végzett adatkezelések jogszerűségét, így különösen, hogy
   - az adatkezelés során az adatkezelés alapelvei érvényesüljenek,
   - az adatkezeléssel érintett személyek adatkezeléssel kapcsolatos jogai biztosításra kerüljenek,
   - az adatkezeléssel érintett személyek személyes adatai ne váljanak nyilvánosan hozzáférhetővé.

b) Biztosítsa a Dandár feladatainak ellátása során keletkező közérdekű adatok nyilvánosságát, a közérdekű adatok megismeréséhez fűződő alapvető jog érvényre juttatását és ezáltal az adatigénylések gyors teljesítését.

c) A honvédelmi adatkezelésekről szóló törvény hatálya alá tartozó adatkezelések tekintetében a honvédelmi adatkezelésekről szóló 2022. évi XXI. törvény (a továbbiakban: Haktv.), a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről szóló, 2016. április 27-i (EU) 2016/679 európai parlamenti és tanácsi rendelet (a továbbiakban: GDPR) 23. cikke szerinti korlátozásokra figyelemmel – az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.),

d) az c) pont hatálya alá nem tartozó adatkezelésekre (a továbbiakban: a GDPR hatálya alá tartozó adatkezelések) a GDPR - az Infotv. 2. § (2) bekezdése szerinti kiegészítésekkel - az irányadó.

2. Értelmező rendelkezések

2. Jelen Szabályzat alkalmazása során a GDPR-ban, valamint a Infotv.-ben meghatározott fogalmak alkalmazandók. Különösen:

a) ***Személyes adat****:* az érintettre vonatkozó bármely információ;

b) ***Érintett:*** bármely információ alapján azonosított vagy azonosítható természetes személy;

c) ***Adatkezelő*****:** az a természetes vagy jogi személy, aki vagy amely:
   - meghatározza a személyes adat kezelésének módját;
   - meghozza a személyes adatok kezelésére vonatkozó döntéseket;
   - végrehajtja vagy az adatfeldolgozóval végrehajtatja a személyes adat kezelésére vonatkozó döntéseket.

d) ***Azonosítható természetes személy:*** az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, azonosító szám, helymeghatározó adat, online azonosító vagy a természetes személy fizikai, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható;

e) ***Különleges adat****:* a személyes adatok különleges kategóriáiba tartozó minden adat, azaz a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a genetikai adatok, a természetes személyek egyedi azonosítását célzó biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok.

f) ***Közérdekű adat:*** 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 hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre, annak eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra és a működést szabályzó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat;

g) ***Közérdekből nyilvános adat****:* a közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli.

h) ***Adatvédelmi incidens:*** az adatbiztonság olyan sérelme, amely a tárolt, továbbított vagy más módon kezelt személyes adatok:
   - véletlen vagy jogellenes elvesztését, megsemmisülését;
   - jogosulatlan továbbítását vagy nyilvánosságra hozatalát;
   - jogosulatlan hozzáférést eredményez.

3. Alapvetések

3. A személyes adatok kezelésének alapelvei:

   a) Jogszerűség, tisztességes eljárás és átláthatóság;
   b) Célhoz kötöttség;
   c) Adattakarékosság;
   d) Pontosság;
   e) Korlátozott tárolhatóság;
   f) Integritás és bizalmas jelleg.

4. A személyes adatok kezelése csak az alábbi jogalapokkal történhet:

   a) Az érintett kifejezett hozzájárulását adta személyes adatainak kezeléséhez;
   b) Az adatkezelés szerződéses kötelezettség teljesítéséhez szükséges;
   c) Az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges;
   d) Az adatkezelés közérdekű feladat végrehajtásához szükséges;
   e) Az adatkezelés egy személy létfontosságú érdekeinek védelme miatt szükséges;
   f) Az adatkezelés az adatkezelő jogos érdekeinek érvényesítéséhez szükséges, de ekkor ellenőriznie kell, hogy az adatkezelés során az érintettek alapvető jogai és szabadságai nem sérülnek-e súlyosan.

4. Az adatkezelő meghatározása

5. Az adatkezelő:

   a) Az adatkezelő megnevezése: Magyar Honvédség Bocskai István 11. Páncélozott Hajdúdandár.
   b) Székhelye: 4027 Debrecen, Füredi út 59-63.
   c) Levelezési cím: 4015 Debrecen, Pf. 50.
   d) Telefonszáma: +36-52/505-200
   e) Elektronikus cím: mh.11.pcttdd@mil.hu
   f) Az adatkezelő képviselője: a Dandár parancsnoka.

5. Az adatvédelmi tisztviselő

6. A Dandár parancsnoka a jelen Szabályzatban meghatározott feladatok érvényesülésének biztosítása, illetve azok ellenőrzése érdekében a Dandár állományából adatvédelmi tisztviselő kijelölésére köteles.

7. Az adatvédelmi tisztviselőnek olyan személyt kell kijelölni, aki:

   a) a személyes adatok védelmére vonatkozó jogi előírások és jogalkalmazási gyakorlat megfelelő szintű ismeretével rendelkezik, vagy azok megszerzésére, elsajátítására - figyelemmel szakmai képzettségére, képességeire - képes;
   b) megfelelő szinten ismeri a Dandár adatkezelési műveleteit, valamint az információbiztonsági és adatvédelmi szabályokat;
   c) megfelelő szinten ismeri a Dandár igazgatási és működési eljárási szabályait;
   d) beosztása nem összeférhetetlen az adatvédelmi tisztviselői tisztség ellátásával.

8. Nem lehet adatvédelmi tisztviselő:

   a) a Dandár parancsnoka, valamint a parancsnokhelyettes;
   b) a Dandár Személyügyi főnöke;
   c) a Dandár Gazdálkodás Támogató és Pénzügyi Ellátó Referatúra vezető pénzügyi referens főtisztje;
   d) a Dandár Jogi és Igazgatási Főnökség főnöke;
   e) a Dandár Híradó és Informatikai Főnökség főnöke;
   f) a Rendszergazda;
   g) a Dandár önálló szervezeti egységeinek - mint adatkezelési művelet végrehajtásáért felelős szervezeti egységek - vezetői.

9. Az adatvédelmi tisztviselőt a Dandár parancsnoka parancsban jelöli ki. Az adatvédelmi tisztviselőként kijelölt személy munkaköri leírásában a tisztviselőként való kijelölést szerepeltetni kell.

10. Az adatvédelmi tisztviselő köteles regisztrálni a Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: NAIH) www.naih.hu honlapján az „Adatvédelmi Tisztviselő Bejelentő Rendszeren”, valamint értesíti a Honvédelmi Minisztérium Jogi Főosztály Adatvédelmi Osztály (a továbbiakban: HM JF AO) osztályvezetőjét. Az értesítés megtörténtéért az adatvédelmi tisztviselőt teszem felelőssé.

11. Az adatvédelmi felelős e tevékenységének ellátása során közvetlenül a Dandár parancsnokának van alárendelve.

12. Az adatvédelmi tisztviselő szakmai elöljárója a HM JF AO osztályvezetője.

13. Az adatvédelmi tisztviselő ezen feladatellátása során nem utasítható az alábbiak tekinteteben:

    a) az adott adatvédelmi kérdéssel kapcsolatos ügyben egy bizonyos álláspont képviseletére;
    b) az adott panasz kivizsgálásának általa meghatározott módjával kapcsolatban;
    c) a NAIH-val való konzultációval kapcsolatban.

14. Az adatvédelmi tisztviselő feladatai:

    a) Bejelenteni az adatkezelőnek való kijelölését a NAIH-nak és a HM JF AO- nak;
    b) Figyelemmel kísérni az adatvédelmi szabályok változásait, önképzés keretében elsajátítani az adatvédelmi területre vonatkozó Európai Uniós és nemzeti jogszabályok előírásait;
    c) Naprakész tanácsokat adni az adatkezelőknek a személyes adatok kezelésével kapcsolatos jogi előírásokról;
    d) Évente egyszer adatvédelmi oktatást tartani a Dandár személyi állománya számára;
    e) Éves jelentést készíteni a HM JF AO számára a Dandár adatvédelmi helyzetéről minden év január 15-ig;
    f) Vezetni a Dandár adatkezeléssel kapcsolatos, az Utasítás által előírt nyilvántartásait;
    g) Ellenőrizni, hogy az adatfeldolgozók tevékenysége megfelel-e az adatvédelmi szabályoknak, az adatfeldolgozók betartják-e a GDPR, a Haktv., az Info.tv., illetve jelen Szabályzat rendelkezéseit (a továbbiakban: adatvédelmi ellenőrzés);
    h) Közreműködni a nem törvény által előírt, új adatkezelésekkel (a továbbiakban: új adatkezelés) kapcsolatos kockázatbecslések, hatásvizsgálat végrehajtásában, szükség esetén ezzel kapcsolatban konzultálni a NAIH-val.
    i) Közreműködni az adatvédelmi tájékoztatók elkészítésében;
    j) Elősegíteni az adatkezeléssel érintett személy adatkezeléssel kapcsolatos jogainak érvényesítését, így különösen kivizsgálni a panaszokat és kezdeményezni az adatkezelőknél a megfelelő intézkedések megtételét;
    k) Közreműködni jelen Szabályzat módosításában, megalkotásában felülvizsgálatában;
    l) Kapcsolatot tartani, konzultálni és szakmai állásfoglalást kérni a NAIH-tól és a HM JF AO-tól;
    m) Részt venni a NAIH és a HM JF AO által szervezett adatvédelmi továbbképzéseken, konferenciákon;
    n) Az érintett adatkezelő irányítása alatt eljáró személyek bevonásával kivizsgálni, és szükség esetén bejelenteni az adatvédelmi incidenseket, ezzel kapcsolatban intézkedéseket javasolni a Dandár parancsnokának;
    o) Feltölteni az egységes közadatkereső rendszerbe a közérdekű, valamint közérdekből nyilvános adatokat;
    p) A Dandárhoz érkezett közérdekű adatigénylések megküldése a HM JF AO-nak, valamint a HM kommunikációért felelős szervének, az azokkal kapcsolatos döntések tervezeteinek elkészítése;

q) A honvédelmi szervezet adatvédelmi feladataira történő teljes körű rálátás biztosítása érdekében az adatvédelmi tisztviselő részt vesz a Dandár vezetői értekezletein.

r) Az adatkezelésekről az alábbi nyilvántartásokat kell vezetni:
   - Adatkezelési tevékenységek nyilvántartása, adatkezelői nyilvántartás;
   - Adatkezelési tevékenységek összesítő nyilvántartása;
   - Adatfeldolgozói tevékenységek nyilvántartása;
   - Adatfeldolgozói tevékenységek összesítő nyilvántartása;
   - Incidensek nyilvántartása;
   - Adatközlési, adattovábbítási nyilvántartás (adatkezelő irányítása alatt eljáró személy vezeti);
   - Az érintett jogainak érvényesítésével kapcsolatos nyilvántartás;
   - Kockázatelemzések, hatásvizsgálatok nyilvántartása;
   - Közérdekű adatigénylések nyilvántartása.

15. Az adatvédelmi tisztviselő jogköre:

Az adatvédelmi tisztviselő – a feladatainak ellátásához szükséges mértékben és célból – jogosult:

a) az adatkezelési nyilvántartásokba betekinteni, az adatkezelőtől az általa folytatott adatkezeléssel kapcsolatban tájékoztatást, felvilágosítást kérni;

b) a tervezett új adatkezelések vonatkozásában közvetlenül feladatot szabni az érintett adatkezelőnek;

c) a közérdekű, valamint közérdekből nyilvános adatok honlapra történő feltétele érdekében közvetlenül feladatot szabni az ilyen adattal rendelkező adatkezelők felé.

6. Az érintett jogai és érvényesítésük

16. A GDPR hatálya alá tartozó adatkezelések esetén - amennyiben a Dandár az érintettől gyűjti be az adatokat – úgy a GDPR 13. cikk szerinti, amennyiben a Dandár nem az érintettől szerzi be az adatokat, úgy a GDPR 14. cikke szerinti tájékoztatót kell az érintett részére bocsátani. A tájékoztató legyen tagolt, közérthető és könnyen értelmezhető. A tájékoztatón túl – a GDPR-ban meghatározott feltételek esetén - biztosítja továbbá az érintett:

a) Hozzáférési jogát;
b) Helyesbítéshez való jogát;
c) Törléshez való jogát;
d) Az adatkezelés korlátozásához való jogát;
e) A tiltakozáshoz való jogát;
f) Automatizált döntéshozatal, profilalkotás esetén az ezzel összefüggő jogát.

17. Az adatkezelő az Info.tv. hatálya alá tartozó adatkezelések esetében – az Info.tv.-ben meghatározott feltételek fennállása esetén – biztosítja az érintett részére:

a) Előzetes tájékozódáshoz való jogát;
b) Hozzáféréshez való jogát;

c) Helyesbítéshez való jogát;
d) Az adatkezelés korlátozásához való jogát;
e) Törléshez való jogát.

18. Az érintett által a GDPR 12. cikk (3) bekezdése, illetve az Infotv. 15. § (1) bekezdés b) pontja szerinti, a Dandár részére az érintett 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.
19. 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.
20. Az érintett által benyújtott kérelemben foglaltakat a lehető legrövidebb időn belül, de legkésőbb a GDPR-ban, illetve az Info.tv.-ben meghatározott határidőn belül kell végrehajtani, és ennek tényéről az érintettet értesíteni.
21. Megalapozatlan vagy egy éven belüli azonos adatkörre vonatkozó kérelem esetén a Dandár díjat számíthat fel a kérelem teljesítésére tekintettel, vagy – kizárólag a GDPR hatálya alá tartozó adatkezelés esetén – a kérelmet elutasíthatja. A költségtérítés alapjául szolgáló díjak vonatkozásában az Utasításban foglaltak az irányadók.

7. Az adatbiztonsággal kapcsolatos feladatok és felelősök meghatározása

22. Az adatbiztonsági és kockázatkezelési előírások részletes meghatározását a honvédelmi tárca információbiztonság politikájáról szóló 94/2009. (XI.27.) HM utasítás 15. és 16. §-ai, valamint a honvédelmi szervezetek általános elektronikus információbiztonsági követelményeinek meghatározásáról és védelmi rendszabályokról szóló 53/2022. (XII.28.) HM utasítás tartalmazza.
23. Az elektronikus információvédelem szabályait a Dandár Elektronikus Információbiztonsági Szabályzata (a továbbiakban: EIBSZ), a nyílt iratok iratkezelési eljárásait a Dandár Iratkezelési Szabályzata tartalmazza.
24. Az adatkezelések során papíralapú és elektronikus dokumentáció keletkezik. Az adatok megőrzési ideje adatkezelésenként kerül meghatározásra. Az adatkezelő, illetve az adatfeldolgozók a megőrzési idő lejártával fizikailag törlik vagy megsemmisítik a személyes adatokat.
25. Az ügyintézők csak azokhoz a személyes adatokat tartalmazó ügyiratokhoz, elektronikus adatállományokhoz férhetnek hozzá, amelyre munkakörük ellátásához szükségük van.
26. A rögzített adatok módosítását csak az arra jogosult felhasználó végezheti el. A módosításkor törekedni kell arra, hogy a módosított adat előzménye megismerhető legyen.
27. Az adat törlését minden esetben az adatért felelős köteles kezdeményezni, a törlésről, megsemmisítésről jegyzőkönyvet kell készíteni.

28. Az adatkezelési művelet végrehajtásáért felelős önálló szervezeti egység vezetőjének minden szükséges intézkedést meg kell tennie annak érdekében, hogy a szervezeti egységnél kezelt személyes adatokkal kapcsolatos adatvédelmi incidens ne történhessen meg. Ennek keretén belül adatkezelési művelet végrehajtásáért felelős önálló szervezeti egység vezetőjének felelőssége, hogy:

    a) azt a helyiséget, amelyben az adatkezelés történik (a továbbiakban: adatfeldolgozó helyiség), úgy alakítsa ki, hogy annak elrendezése meggátolja az adatvédelmi incidens bekövetkezését;
    b) az adatkezelés során csak azon személyes adatot tartalmazó irat maradjon az asztalon, amellyel az adatkezelő irányítása alatt eljáró személy érdemi munkát végez;
    c) amennyiben az adatok megismerésére nem jogosult személy lép az adatfeldolgozó helyiségbe, úgy megóvja a személyes adatot tartalmazó iratot az illetéktelen megismeréstől;
    d) az adatfeldolgozó helyiségben a személyes adatokat tartalmazó iratok ne kerüljenek kifüggesztésre, valamint egyéb olyan módon tárolásra, amely azok illetéktelen személy általi megismerését eredményezheti;
    e) az adatfeldolgozó helyiséget - amennyiben azt az adatkezelő irányítása alatt eljáró személy elhagyja - bezárja;
    f) a személyes adatot tartalmazó iratok tarolása zárható íróasztalban, szekrényben, illetve páncélszekrényben történjen;
    g) a személyes adatokat tartalmazó iratokat a szolgálatteljesítési idő befejeztével az adatkezelő irányítása alatt eljáró személy köteles a fenti tarolási helyeken elzárni.

29. Személyes adatot tartalmazó iratot a szolgálatteljesítési helyről kivinni, valamint azon kívül tanulmányozni, feldolgozni, tárolni csak adatkezelési művelet végrehajtásáért felelős önálló szervezeti egység vezetője engedélyével lehet. Az engedélyben rögzíteni kell:

    a) a kivitelre jogosult személy nevét;
    b) a munkahelyről kivihető iratok iktatási-, nyt. számát, példányszámát;
    c) az irat munkahelyen kívüli tanulmányozásának időtartamát.

8. Adatvédelmi incidensek kezelése, jelentése

30. **Adatvédelmi incidens:** A biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi.

31. A honvédelmi szervezet az EU Rendelet 33. cikk (1) bekezdésében és az Infotv. 25/J. § (1) bekezdésében meghatározottakat megelőzően, a bekövetkeztéről való tudomásszerzést követő legfeljebb 24 órán belül köteles az adatvédelmi incidenst bejelenteni a szakmai szerv részére az adatvédelmi tisztviselő által.

32. Adatvédelmi incidens gyanúja esetén az adatvédelmi tisztviselőt haladéktalanul értesíteni kell és részére a releváns információkat megadni. Az adatvédelmi tisztviselő a lehető

legtöbb információt összegyűjti az incidens munkacsoport (a továbbiakban: IMCS) számára, majd ésszerű határidőn belül összehívja az IMCS tagjait.

33. Az IMCS tagjai:

    a) olyan adatkezelés esetén, amely során minősített adatok és rendszerek érintettek, a biztonsági vezető (vagy helyettes biztonsági vezető),
    b) az adatvédelmi tisztviselő,
    c) az incidenssel érintett szervezeti elem vezetője,
    d) elektronikus adatkezelés esetén a Híradó és Informatikai Főnökség informatikai tisztje.

34. Az IMCS haladéktalanul megkezdi az adatvédelmi incidens kivizsgálását, megvizsgálja, hogy:

    a) a biztonság sérülése érinti-e a személyes adatok biztonságát,
    b) kockázatos-e a biztonság sérülése az érintettek jogaira és szabadságaira nézve, különös tekintettel az 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 érintettek értesítése.

35. Amennyiben az IMCS az eseményt adatvédelmi incidensként értékeli, úgy dönt annak alacsony, közepes vagy magas kockázatáról. Az IMCS a döntéséről az adatvédelmi incidens bekövetkeztéről való tudomásszerzést követő 24 órán belül értesíti a szakmai szervet.

36. Az adatvédelmi incidens lehet alacsony, közepes vagy magas kockázatú. Alacsony kockázatú adatvédelmi incidenst kizárólag az adatvédelmi incidens nyilvántartásban szükséges rögzíteni.

37. Ha az adatvédelmi incidens közepes vagy magas kockázatú, az IMCS javaslatot tesz az adatkezelő részére az adatvédelmi incidens következményeinek mérséklését célzó intézkedésekre. Ezekben az esetekben az adatvédelmi incidenst az adatvédelmi tisztviselő az adatkezelő képviselőjének tudomásszerzésétől számított 72 órán belül bejelenti a NAIH részére annak incidensbejelentő rendszerén keresztül. Magas kockázatú adatvédelmi incidens bekövetkeztéről az érintetteket - a megfelelő intézkedés megtétele céljából - tájékoztatni kell. A tájékoztatás megtételéről az adatvédelmi tisztviselő - távolléte esetén a helyettesítésére kijelölt személy - gondoskodik.

9. Hatásvizsgálat és kockázatbecslés

38. Az adatkezelést megelőzően az érintett adatkezelési művelet végrehajtásáért felelős önálló szervezeti egység a tervezett adatkezelés kockázatainak megállapítása érdekében előzetes kockázatértékelést végez, amelynek eredményéről tájékoztatja az adatvédelmi tisztviselőt. Az adatvédelmi tisztviselő szakmai tanácsadást nyújt az adatvédelmi hatásvizsgálat elvégzéséhez, valamint nyomon követi az elkészítését.

39. 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.

40. A kockázatbecslést a HM JF AO által biztosított excel táblázat alapján kell végrehajtani, amely az adatvédelmi tisztviselőnél megtalálható.

41. A hatásvizsgálat tartalmazza:
    a) az adatkezelői műveletek általános leírását;
    b) az érintettek alapvető jogainak érvényesülését fenyegető, azonosított kockázatok leírását és jellegét;
    c) a kockázatok kezelése céljából tervezett, illetve alkalmazott intézkedéseket.

42. Amennyiben a hatásvizsgálat magas kockázatot állapít meg, és a feltárt kockázatok megfelelő intézkedésekkel nem csökkenthetők, az adatvédelmi tisztviselő a NAIH-val történő konzultációt megelőzően egyeztet a szakmai szervvel. A hatásvizsgálat megfelelő lezárásáig az adatkezelést nem lehet megkezdeni.

43. Az adatvédelmi tisztviselő köteles intézkedni arra nézve, hogy a NAIH által feltárt hiányosságok megszüntetésre, és az általa javasolt intézkedések bevezetésre kerüljenek a tervezett adatkezelés vonatkozásában.

44. A NAIH által megállapított hiányosságok kiküszöböléséről, valamint az általa javasolt intézkedések megtételéről az adatvédelmi tisztviselő köteles a NAIH-t írásban értesíteni.

45. A tervezett adatkezelés csak a NAIH engedélyét követően kezdhető meg. Az engedélyezett adatkezelésről az adatvédelmi tisztviselő adatvédelmi tájékoztatót készít.

10. Adatközlés, adattovábbítás

46. Az érintett személyes adatainak közlésére, továbbítására kizárólag jelen Szabályzatban meghatározottak szerint és 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 az adatközlést, adattovábbítást megengedi és az adatkezelés feltételei minden egyes személyes adatra nézve teljesülnek;
    c) az adattovábbítás 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.

47. Az adatvédelmi tisztviselő szakmai véleményét minden adatközlést, adattovábbítást megelőzően ki kell kérni, kivéve azokat az adatközléseket, adattovábbításokat, melyeket jogszabály kötelezően előír.

11. Az elektronikus közzététel szabályai

48. Az adatkezelő honvédelmi szervezet köteles csatlakozni az egységes közadatkereső rendszerhez, melybe feltölti az Infotv. 37/B. §-ában meghatározott adatokat.
49. Az egységes közadatkereső rendszerhez csatlakozáskor kapcsolattartónak a honvédelmi szervezet tekintetében az adatvédelmi tisztviselő minősül.
50. Az egységes közadatkereső rendszerbe adatok feltöltésére akkor kerülhet sor, ha a szakmai szerv azok feltöltésével előzetesen egyetértett.
51. Az adatkezelő az általános közzétételi listában meghatározott, a felelősségi körébe tartozó adatokat, illetve azok változását a változás elrendelésének vagy megtörténtének napján, elektronikus úton, a szakmai szervnek megküldi, mely a szakmai vizsgálatot követően a HM adatközlőnek továbbítja közzétételre.
52. A Központi Információs Közadat-nyilvántartás elektronikus felületen történő adatszolgáltatást az adatvédelmi tisztviselő bevonásával a Dandár hivatali tárhelyéről kell végrehajtani az Infotv. 37/C § (2) bekezdésében meghatározott kéthavi rendszerességgel. Az Adatlapon feltüntetett adatok teljességéért és valóságnak való megfelelőségéért a Dandár Logisztikai és Gazdálkodási Alosztály Gazdálkodási Részlege tartozik felelősséggel. Az adatvédelmi tisztviselő kötelessége a feltöltésre tervezett adatlap tartalmi szempontú jóváhagyásra történő felterjesztése a HM JF AO részére.

12. Közérdekű adatigénylés teljesítésének rendje

53. A közérdekű adat megismerése iránti igény teljesítése során a Dandár az Info.tv-ben meghatározott határidők betartásával és az Utasításban meghatározott eljárási rend szerint, az alábbi részletszabályok figyelembevételével jár el.
54. Közérdekű adat igénylése történhet:
    a) szóban,
    b) írásban: parpírlapon vagy elektronikus formában.
    A szóban bejelentett igényt az adatvédelmi tisztviselőnek a szóbeli bejelentéskor írásba kell foglalnia.
55. Az adatvédelmi tisztviselő köteles az igényt a kézhezvételt követően haladéktalanul elektronikus úton megküldeni a HVK JIF útján a HM JF AO, illetve a HM kommunikációért felelős szerv részére.

56. Az igényléssel érintett közérdekű adattal rendelkező szervezeti elem vezetője köteles minden információt megadni az adatvédelmi tisztviselő részére az igénylés teljesítése vagy a teljesítés elutasítása érdekében.

57. A honvédelemről és a Magyar Honvédségről szóló 2021. évi CXL. törvény (a továbbiakban: Hvt.) 15.§ (1) bekezdése alapján **a honvédelmi szervezetek személyi állományára vonatkozó** – a Honvédség védelmi képességének, hadrafoghatóságának biztosításával összefüggő – **adatok honvédelmi és nemzetbiztonsági érdekből a keletkezésüktől számított 30 évig nem nyilvánosak**. Ezen adatok megismerését a fenti érdekek mérlegelésével a Dandár tekintetében a Honvéd Vezérkar Főnöke engedélyezheti.

58. A Hvt. 15. § (3) bekezdése alapján **a honvédelmi szervezet felépítésére, működésére, haditechnikai eszközeire és anyagaira, valamint hadfelszerelésére vonatkozó adatok honvédelmi és nemzetbiztonsági érdekből keletkezésüktől számított 30 évig nem nyilvánosak.** Ezen adatok megismerését a fenti érdekek mérlegelésével a Dandár tekintetében a Honvéd Vezérkar Főnöke javaslatára a honvédelemért felelős miniszter engedélyezheti.

59. A Dandárparancsnok a megkeresésre írt válasz tervezetét a beérkezést követő 3 munkanapon belül felterjeszti a HVK JIF útján a HM JF AO, a HM kommunikációjáért felelős szerv és az MHPK részére, melyek a választervezettel kapcsolatos álláspontjukról haladéktalanul tájékoztatják a megküldőt.

60. A választervezetet, továbbá a HM JF AO és a HM kommunikációjáért felelős szerv, valamint a HVKF álláspontját a szolgálati elöljárók egyidejű tájékoztatása mellett - a beérkezést követő 5 munkanapon belül - jóváhagyás céljából, a HM kabinetfőnök részére küldi meg.

61. A jóváhagyott választervezetet a Dandárparancsnok megküldi az igénylő részére azzal, hogy azt a HVK JIF útján a HM JF AO részére is meg kell küldeni.

62. Amennyiben az igényelt adat kezelője nem a Dandár, úgy az igényt a kézhezvétel napján köteles továbbítani a közérdekű adatot kezelő szervnek. Az igény áttételéről egyidejűleg tájékoztatni kell az adatigénylőt. Abban az esetben, ha az illetékes szerv nem állapítható meg, az adatigénylőt az igény teljesíthetetlenségéről kell értesíteni.

63. A jóváhagyás alapján teljesített vagy elutasított kérelmeket az adatvédelmi tisztviselő nyilvántartásba veszi.

64. Az adatvédelmi tisztviselő a tárgyévet követő év január 31-ig tájékoztatja a NAIH-ot az elutasított adatigénylésekről és az elutasítás indokairól.

13. A közérdekű adatigénylés teljesítéséért megállapítható költségtérítés

65. A Dandárparancsnok az adatigénylés teljesítéséért az Infotv. 29. § (3) és (4) bekezdésében, 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.

66. A választervezetet kidolgozó előzetesen megbecsüli a munkára fordítandó munkaidőt és a felmerülő dologi kiadások összegét, ezt haladéktalanul megküldi az adatvédelmi tisztviselő részére.

67. Amennyiben az adatvédelmi tisztviselő megállapítja, hogy az Infotv. 29. § (3) bekezdése alapján költségtérítés felszámolásának van helye, 15 napon belül tájékoztatja az igénylőt a költségtérítés összegéről, valamint az adatigénylés teljesítésének a másolatkészítést nem igénylő lehetőségeiről. Ezen tájékoztatás kézhezvételét követő 30 napon belül nyilatkozik az igénylő arról, hogy az igényét fenntartja-e. A tájékoztatás megtételéről az igénylő nyilatkozatának a Dandárhoz való beérkezéséig terjedő időtartam az adatigénylés teljesítésére rendelkezésre álló határidőbe nem számít bele.

68. A tájékoztatáshoz csatolni kell egy az adatigénylő költségtérítés megfizetésének teljesítéséhez szükséges személyes adatainak megadására vonatkozó nyomtatványt (a közérdekű adatigénylés tárgyának megjelölése, az adatigénylő neve, címe, számlázási neve, számlázási címe) és az adatigénylőt fel kell kérni arra, hogy a tájékoztatást követő igénylésének fenntartása esetén azt megfelelően kitöltve küldje vissza.

69. Ha az adatigénylő a tájékoztatás kézhezvételétől számított 30 napon belül nyilatkozik adatigénylésének fenntartásáról, akkor a válaszadásra kötelezett legalább 15 napos határidőt határoz meg a költségtérítés megfizetésére.

70. A válaszadásra kötelezett az adatigénylést a költségtérítésnek az adatigénylő általi megfizetését követő 15 napon belül teljesíti.

71. A felszámítható költségek mértékét a HM hivatalos honlapján közzétett hirdetmény tartalmazza. A költségtérítéssel kapcsolatos számla kibocsátása az Gazdálkodás Támogató és Pénzügyi Ellátó Referatúra feladata. A költség adatigénylő általi megfizetésének tényét Gazdálkodás Támogató és Pénzügyi Ellátó Referatúra haladéktalanul jelzi a válaszadásra kötelezettnek.

72. Az alcímben nem szabályozott esetekben a Korm. rendeletben meghatározottak szerint kell eljárni, figyelembe véve a HM fejezet egységes számviteli politikájáról és számlarendjéről szóló 33/2021. (HK 1/2022.) HM KÁT szakutasítás rendelkezéseit.

14. A képrögzítésre alkalmas elektronikus megfigyelőrendszerrel kapcsolatos nyilvántartás

73. A honvédelmi szervezet az objektumban képrögzítésre vagy kép- és hangrögzítésre alkalmas elektronikus megfigyelőrendszert telepíthet, amely alkalmazásával az objektumban, valamint annak közvetlen környezetében tartózkodó személyekről felvételt készíthet az élet- és vagyonbiztonság, valamint a minősített adatok védelme érdekében. Az adatokat a kép-, illetve a kép- és hangrögzítésre alkalmas elektronikus megfigyelőrendszert alkalmazó honvédelmi szervezet kezeli. Az objektum őrzését ellátó megbízás alapján az adatokat rögzítheti és tárolhatja, e tekintetben adatfeldolgozónak minősül, az adatfeldolgozás feltételeit szerződés tartalmazza.

74. A kép-, illetve a kép- és hangrögzítésre alkalmas elektronikus megfigyelőrendszer alkalmazása esetén jól látható helyen az elektronikus megfigyelőrendszer alkalmazására utaló figyelemfelhívó jelzést és adatkezelési tájékoztatót kell elhelyezni.

75. Nem alkalmazható kép-, illetve kép- és hangfelvétel rögzítésére alkalmas elektronikus megfigyelő rendszer olyan helyen, ahol a megfigyelés az emberi méltóságot sérti, különösen öltözőben, mosdóban, illemhelyen, a személyi állomány pihenésére rendelt helyiségekben, illetve betegellátást végző helyiségben.

76. A rögzített kép-, illetve kép- és hangfelvételt a rögzítéstől számított 30 napig kell tárolni, azt követően haladéktalanul törölni kell.

77. Ezen időtartamon belül az adatkezelő a rögzített kép-, illetve kép- és hangfelvételt a jogszabályban meghatározott szabálysértési, igazságszolgáltatási és fegyelmi eljárás, büntetőeljárás vagy más hatósági eljárás lefolytatása céljából az előkészítő eljárást folytató szerv, a nyomozó hatóság, a szabálysértési hatóság, a fegyelmi ügyben eljáró szerv, az ügyészség, a bíróság, vagy más hatóság, a törvényben meghatározott feladatai ellátása céljából a nemzetbiztonsági szolgálat, valamint az érintett jogainak gyakorlása céljából, az érintett részére továbbítja.

78. Az, akinek jogát vagy jogos érdekét a kép-, illetve a kép- és hangfelvétel rögzítése érinti, az 77. pontban megjelölt eljárás lefolytatásához kérheti, hogy az adatot annak kezelője az adat továbbításáig ne törölje. A kérelem benyújtására a kép-, illetve a kép- és hangfelvétel rögzítésétől számított 30 napon belül van lehetőség. Bíróság, ügyészség, nyomozó hatóság vagy más hatóság adatszolgáltatás-kérésére a rögzített kép-, illetve kép- és hangfelvételt haladéktalanul meg kell küldeni. Ha a kérelem benyújtásától számított 30 napon belül nem kerül sor megkeresésre, a rögzített kép-, illetve kép- és hangfelvételt törölni kell.

79. A kezelt személyes adatok gyűjtésének forrása: az érintett.

15. Adatvédelmi oktatás

80. Az adatvédelmi tisztviselő a Dandár teljes személyi állománya részére évente legalább egyszer adatvédelmi oktatást tart. Az oktatás témáiról az adatvédelmi tisztviselő foglalkozási jegyet készít.

81. Az adatvédelmi oktatás megtartható jelenléti oktatással, illetve elektronikus formában.

82. A jelenléti oktatást az EIBSZ oktatásával egyidőben kell megtartani az oktatás végén vizsgát kell tartani, amely szóban, visszakérdezéssel valósul meg.

83. Elektronikus formában végrehajtott oktatás esetén az adatvédelmi tisztviselő az oktatási anyagot Outlook-on megküldi az alegységparancsnokok illetve az önálló szervezeti elemek vezetői részere Az alegységparancsnokok és önálló szervezeti elemek vezetői az előadás anyagát ismertetik az állománnyal, majd az ismertetés(ek)en résztvevők névsorát tartalmazó jelenléti íveket átadjak az adatvédelmi tisztviselőnek annak dokumentálása céljából.

16. Az adatvédelmi tisztviselő ellenőrzési feladatai

84. Az adatvédelmi tisztviselő minden év november 15-ig ellenőrzési tervet készít, melyet a Dandárparancsnok hagy jóvá. Az ellenőrzési tervet úgy kell elkészíteni, hogy valamennyi szervezeti elem, alegység ellenőrzésére sor kerüljön.

85. Az adatvédelmi tisztviselő az ellenőrzéseit a tervnek megfelelően köteles végrehajtani, azok eredményéről jelentést készít a Dandárparancsnok részére.

17. Az adatvédelmi ellenőrzés

86. Az adatvédelmi ellenőrzés célja: a Dandár szervezeti elemeinél, alegységeinél az adatvédelmi jogszabályok, illetve belső szabályzatok betartásának ellenőrzése.

87. Az adatvédelmi ellenőrzés főbb szempontjai:

a) az adatkezelés személyi feltételeinek ellenőrzése, az adatkezelést végző személyek felkészültsége, leterheltsége;
b) az adatkezelés tárgyi feltételeinek biztosítása;
c) az elektronikus és papíralapú adathordozók tárolása, biztonsága;
d) az adatkezelés módja;
e) a szervezeti elemhez, alegységhez érkezett adatvédelmi megkeresésekre adott válaszok jogszerűsége;
f) egyéb, adatvédelmet érintő rendszerek, különösen a beléptető, a zárt láncú kamera, valamint az elektronikus nyilvántartási rendszerek üzemeltetésének jogszerűsége.

88. Az adatvédelmi tisztviselő az ellenőrzés során jogosult:

a) a nyilvántartásokba való betekintésre;
b) az adatkezeléssel kapcsolatban felvilágosítást, tájékoztatást kérni;
c) az adatkezeléssel és az adatbiztonsággal kapcsolatos azonnali intézkedésre okot adó esemény észlelése esetén - annak megszűntetése érdekében - javaslatot tenni az ellenőrzött szervezeti elem vezetőjének.

89. Az adatvédelmi tisztviselőnek az adatvédelmi ellenőrzést úgy kell végrehajtania, hogy az az ellenőrzött szervezeti elem napi tevékenységét a lehető legkisebb mértékben zavarja.

90. Az ellenőrzött szervezeti elem vezetője köteles az adatvédelmi tisztviselő munkáját segíteni, az általa kért tájékoztatásokat a valóságnak megfelelően, a lehető legrövidebb időn belül megtenni.

91. A kamerás megfigyelő rendszerekhez kapcsolódó adatvédelmi ellenőrzés főbb szempontjai:

a) az adatvédelmi tájékoztató piktogramok megléte;
b) az adatvédelmi piktogramok állapota, olvashatósága;
c) az adatkezelési tájékoztatók megléte.

18. Záró rendelkezések

92. Jelen Szabályzat 2024. augusztus 15-én lép hatályba, mellyel egyidejűleg a Magyar Honvédség Bocskai István 11. Páncélozott Hajdúdandár parancsnokának Adatvédelmi és Adatbiztonsági 687/646. nyilvántartási számú Szabályzata hatályát veszti.

93. A Szabályzatot az adatkezelés körülményeiben beállt lényeges változás esetén, de legalább évente felül kell vizsgálni. A felülvizsgálatot az adatvédelmi tisztviselő végzi el.

94. A Szabályzatot a Dandár önálló szervezeti egységeinek vezetői és az alegységparancsnokok teljes terjedelmében ismerjék meg, az alárendelt személyi állományukkal a rájuk vonatkozó mértékben ismertessék meg.