



JÁSZ-NAGYKUN-SZOLNOK MEGYEI BÜNTETÉS-VÉGREHAJTÁSI INTÉZET

---

Jóváhagyom:

Horváth Ákos bv. alez.  
büntetés-végrehajtási tanácsos  
intézetparancsnok

A Jász-Nagykun-Szolnok Megyei Büntetés-végrehajtási Intézet - személyes adatokra vonatkozó -

## **Adatvédelmi és adatbiztonsági szabályzata**

Készítette: Kelemen Richárd bv. alez., bv. tanácsos  
Készült: 2017. augusztus 31-én, 1 pld. eredetben  
Található: FAL/Szabályozások/Dokumentációk elektronikus mappában

## **I. Általános rendelkezések**

1. A büntetés-végrehajtási szervezetről szóló 1995. évi CVII. törvény 4. § (2) c) pontja, a büntetések, az intézkedések, egyes kényszerintézkedések és a szabálysértési elzárás végrehajtásáról szóló 2013. évi CCXL. törvény (a továbbiakban: Bv. tv.), valamint az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Info.tv.) 24. §-ának (3) bekezdése, az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény, az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezelésének egyes kérdéseiről 62/1997. (XII. 21.) NM rendelet, valamint a büntetés-végrehajtási szervezet 52/2017. számon kiadott Adatvédelmi és Adatbiztonsági Szabályzata (továbbiakban: Szabályzat) alapján, a Jász-Nagykun-Szolnok Megyei Büntetés-végrehajtási Intézet (továbbiakban: Intézet) által kezelt személyes adatok védelme érdekében, az adatvédelemre és adatkezelésre vonatkozó jogszabályok, illetve szabályzók végrehajtására kiadom az Intézet adatkezelési szabályzatát.
2. A helyi szabályzat hatálya nem terjed ki a közérdekű adatokra.
3. Az Intézet belső adatvédelmi felelősének Kelemen Richárd bv. alezredes, bv. tanácsost jelölöm ki, feladatait kapcsolt munkakörben látja el. Feladatait a munkaköri leírása tartalmazza.
4. Az adatvédelmi felelős feladatait az Info.tv.24. § (2) bekezdése alapján látja el. Az adatvédelmi felelős feladata továbbá, az adatkezelési szabályzat szükséges módosításának, aktualizálásának előkészítése.
5. Az adatkezelési rendelkezéseket mind a manuális, papír alapú, mind az elektronikus adatkezelés során érvényre kell juttatni.
6. Az adatkezelésnek az adatkezelés minden fázisában meg kell felelnie a jogszabályokban meghatározott követelményeknek.
7. Az intézkedést, valamint a személyes, a különleges- és egészségügyi adatok védelméről szóló jogszabályokat a teljes személyi állománnyal ismertetni kell, azt oktatások során kellő rendszerességgel fel kell dolgozni.
8. Az intézetben a technikai ellenőrzések végrehajtása érdekében, a 2013. évi CCXL. tv. 150. §-a alapján elektronikus megfigyelő rendszer üzemel.

## **II. Részletes rendelkezések**

### **Az adatkezeléssel kapcsolatos nyilvántartások**

9. Az adatkezeléssel kapcsolatos intézeti nyilvántartásokat a Szabályzat mellékleteinek megfelelő formátumban kell felfektetni.
10. Az Intézet által kezelt, személyes adatot tartalmazó nyilvántartásokról adatvédelmi nyilvántartást kell vezetni. Az Intézet belső adatvédelmi nyilvántartását az adatvédelmi felelős vezeti, a személyes adatot kezelő szervezeti egység vezetőjének bejelentése alapján.

11. Az Intézet szakterületein adattovábbítási nyilvántartást kell vezetni, amelyhez csak az adott szakterület adatkezelésre jogosult személyei és az intézet adatvédelmi felelőse férhet hozzá. Az intézeti adatvédelmi felelős az intézeti szinten összesített adattovábbítási nyilvántartáshoz is hozzáfér. Az adattovábbítási nyilvántartás fenti módon való kialakításáért az informatikai osztályvezető a felelős.
12. A szakterületi vezető felelős a betekintési nyilvántartás vezetéséért.
13. Az intézethez érkezett tájékoztatási kérelmek jogosultságát minden esetben az érintett szakterület vizsgálja meg, amelynek végrehajtásáért a szakterületi vezető a felelős. A megkeresésekre adott válaszok parancsnoki jóváhagyásra történő előkészítése a nyilvántartást vezető szervezeti egység vezetőjének a feladata. Az adatvédelmi tárgyú, személyes adatra vonatkozó megkeresések érdemi megválaszolása során a Szabályzat 23. és 24. pontjaiban meghatározott határidők betartásáért a szakterületi vezető felelős.
14. A személyes adatokat tartalmazó adatállományok dokumentációnak nyilvántartásba vételéért az adott szervezeti egység vezetője a felelős. A dokumentációkhoz való hozzáférés jogosultságát a jogosult személy munkaköri leírásában kell rögzíteni.

### **A helyi belső adatvédelmi felelős feladat- és hatásköre**

15. A személyes adatot kezelő szervezeti egység vezetőjének bejelentése alapján vezeti a belső adatvédelmi nyilvántartást.
16. Vezeti az intézet adatvédelmi nyilvántartását.
17. Közreműködik, illetve segítséget nyújt az adatkezeléssel összefüggő döntések meghozatalában.
18. Ellenőrzi a mindenkor hatályos információs önrendelkezési jogról és az információszabadságról szóló törvény és az adatkezelésre vonatkozó más jogszabályok, valamint a belső adatvédelmi és adatbiztonsági szabályzatok rendelkezéseinek és az adatbiztonsági követelményeknek a megtartását.
19. Gondoskodik az adatvédelmi ismeretek oktatásáról.
20. Elkészíti az intézet adatvédelmet érintő belső normáinak tervezetét.

Segíti az adatkezelésre vonatkozó jogszabályok és belső normák érvényre juttatását, figyelemmel kíséri az adatvédelemmel összefüggő jogszabály-változásokat, részt vesz az intézetparancsnok adatvédelmi tárgyú döntéseinek előkészítésében. Állásfoglalás kialakításával, véleményezéssel segíti az intézet adatvédelmi munkáját.

21. Kivizsgálja az intézet adatkezelésével összefüggésben érkező panaszokat, kifogásokat, közreműködik, illetve segítséget nyújt az érintettek jogainak gyakorlásában. Jogosulatlan adatkezelés észlelése esetén annak megszüntetésére hívja fel az adatkezelőt vagy az adatfeldolgozót.
22. Az intézetparancsnok megbízásából ellenőrzi az intézetnél az adatvédelmi követelmények megtartását, az előírások megszegésének észlelése esetén felhív a jogszerű állapot haladéktalan helyreállítására. A hiányosságokat jelzi az intézetparancsnok részére, indokolt esetben javaslatot tesz a felelősség megállapításához szükséges eljárás lefolytatására.

23. Köteles részt venni a központi oktatáson, gondoskodik az ott elhangzott ismereteknek az intézet személyi állománya részére történő továbboktatásáról.
24. A BVOP Adatvédelmi és Adatbiztonsági Szabályzata alapján elkészíti az adatvédelmi tevékenységéről szóló jelentéseket és adatszolgáltatásokat.

### **A helyi adatvédelem rendszere, védelmi intézkedések**

25. A személyi állomány tagjai a munkaköri vagy szolgálati feladatuk ellátáshoz szükséges adatbázisokhoz és nyilvántartásokhoz férhetnek hozzá. A jogosultság megállapítására alapot adó körülményekben változás történik a szakterületi vezető haladéktalanul intézkedni köteles a jogosultság módosításra vagy visszavonására.
26. A Szabályzat 69. pontja alapján, a szakterületi vezető kötelez a jogosultat írásban tájékoztatni.
27. A személyi és fogvatartotti állománnyal kapcsolatosan használt személyes adatokat az adatkezelők csak a munkájukhoz szükséges mértékben használhatják, azt magáncélra felhasználni tilos.
28. Telefonon történő, továbbá személyes megkeresés esetén személyes adatot kiadni tilos, csak hivatalos írásbeli megkeresés alapján, az adatvédelmi jogszabálynak megfelelően, dokumentálva engedélyezett,
29. A személyi állományi tagok a fogvatartottakkal való érintkezése a Szolgálati Szabályzatban meghatározottaknak megfelelően, csak a hivatalos szolgálati tevékenységre irányulhat, velük magánbeszélgetést folytatni, illetve előttük szolgálati vagy magánügyeiket megbeszélni tilos.
30. Az adatok kezelése során biztosítani kell az adatok biztonságát véletlen vagy szándékos megsemmisítéssel, megsemmisüléssel, megváltoztatással, károsodással, nyilvánosságra kerüléssel szemben, továbbá, hogy azokhoz illetéktelen személy ne férjen hozzá.
31. A személyes adatok védelme érdekében a személyes adatokat tartalmazó iratokat, arra rendszeresített, zárható szekrényekben, asztalfiókokban kell elhelyezni, azokat kulccsal le kell zárni, a kulcsokat az iroda számozott kulcsdobozában kell elhelyezni.
32. Munkaidőn kívül, személyes adatot tartalmazó vagy arra utaló iratot, dokumentumot, egyéb információt elzáratlanul (pl.: asztalon, szekrényen stb.) nem lehet hagyni. Munkaidőn kívül zárva kell tartani az asztalok fiókjait és egyéb dokumentumokat tartalmazó szekrényeket is.
33. A kulcsdobozt csak az azon feltüntetett személyek vehetik fel, illetve takarítás céljából munkaidőn túl csak a takarító személyzet rendelkezhet bejárással a takarítási feladatok elvégzéséig. Az egyes helyiségek zárására, a kulcsok tartására és kezelésére vonatkozó helyi rendelkezéseket maradéktalanul be kell tartani. Amennyiben a szakterület dolgozója nem tartózkodik az irodában, azt kulcsra zárva kell tartani, oda más nem léphet be a távollétében. Nem a szakterület állományába tartozó személynek az irodába történő belépése és ott-tartózkodása csak az osztály dolgozóinak jelenlétében engedélyezett.
34. A számítógép monitorját úgy kell elhelyezni az irodában, hogy a belépő személy azt ne láthassa, információ ne kerüljön a birtokába. Bejelentkezett számítógépet őrizetlenül hagyni nem lehet.
35. A munkavégzés során keletkezett rongtolt vagy fel nem használt személyes adatokat tartalmazó adathordozókat meg kell semmisíteni. Az adathordozók megsemmisítést oly módon kell végrehajtani, hogy abból adat ne legyen kinyerhető.

## **A személyes adatok veszélyhelyzetben történő védelme**

36. Rendkívüli esemény, veszélyhelyzet, katasztrófa helyzet esetén, illetőleg következményeinek az elhárítása során a kár elhárítására feladat- és hatáskörrel rendelkező szervek, valamint a biztonsági vezető és adatvédelmi felelős értesítése mellett az emberi élet veszélyeztetése nélkül egyidejűleg meg kell kezdeni a kár felszámolását. A kár elhárítása, felszámolása során is fokozott figyelmet kell fordítani arra, hogy illetéktelen személyek ne férhessenek a személyes adatokhoz.
37. Amennyiben emberi élet veszélyeztetése nélkül megoldható, meg kell kezdeni a veszélyeztetett adathordozók, valamint biztonsági területen tárolt veszélyeztetett minősített adathordozók mentését és biztonságos helyre szállítását. Az iratok megfelelő őrzésének megszervezéséről az érintett szakterületi vezető a biztonsági osztályvezetővel együttműködve köteles gondoskodni.
38. Az adathordozók szállítási módját minden esetben az adatvédelmi felelős és az érintett szakterületi vezető közösen határozza meg, oly módon, hogy az adatokhoz illetéktelenek ne férhessenek hozzá.
39. Minősített adatok tekintetében az intézet minősített adatok védelmére kiadott Biztonsági Szabályzatában foglaltaknak megfelelően kell eljárni.
40. A kár elhárítása után a szakterületi vezetők kötelesek felmérni, hogy történt-e adatvesztés. A felmérés eredményéről a szakterületi vezető tájékoztatja az adatvédelmi felelőst és jelentést tesz intézetparancsnok részére.

### **Kamerahasználat**

41. Az intézetben telepített videokamerás megfigyelő rendszer képeket a rendszer a jogszabályi előírásnak megfelelően 30 napig automatikusan rögzíti. Az intézet külső, közterületi megfigyelésére telepített kamerák a felvételeket a rögzítést követő három napig őrzik meg. A technikai rendszer megfelelő beállításáért az informatikai osztályvezető felel.
42. A kameraképek archiválása során – a Bv. Kódex 150. §-ában foglaltaknak megfelelően – a vonatkozó OP szakutasításban foglaltaknak alapján kell eljárni. A rendszerben tárolt adatok archiválása csak intézetparancsnoki engedéllyel lehetséges. Az archiválás végrehajtásáért az informatikai osztályvezető a felelős.
43. Az elektronikus megfigyelési eszközök alkalmazásának egyéb szabályait, és az elektronikus megfigyelési eszközön ellenőrzési tevékenységre kötelezettek „Az intézet biztonságtechnikai rendszere” és „A technikai jelzőrendszer működtetése, az elektronikus megfigyelő eszköz felvételeinek ellenőrzése” tárgyában kiadott intézetparancsnoki intézkedések tartalmazzák.
44. Az intézet minden bejáratánál jól láthatóan elhelyezett, olvasható felirattal (táblával) fel kell hívni a figyelmet arra, hogy kamerarendszer működik és a felvételek rögzítésre kerülnek. A táblák kihelyezéséért és esetleges pótlásukért a gazdasági vezető a felelős.