



III. AGGLOMERÁCIÓ
KALOCSAI FEGYHÁZ ÉS BÖRTÖN

A KALOCSAI FEGYHÁZ ÉS BÖRTÖN PARANCSNOKÁNAK

INTÉZKEDÉSE

Tárgy: A Kalocsai Fegyház és Börtön adatkezelése

Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Info.tv.) 25/A.§ (3), 30.§(6), valamint 35.§ (3) bekezdésében foglaltak, valamint a büntetés-végrehajtás országos parancsnokának „a büntetés-végrehajtási szervezet adatvédelmi és adatbiztonsági szabályzatáról, valamint a közérdekű adatok megismerésének és közzétételének rendjéről szóló 25/2025 (XL.20.) BVOP utasítása (a továbbiakban: Utasítás), továbbá a büntetés-végrehajtás országos parancsnokának „egyes BVOP utasítások módosításáról szóló 22/2022 (IX.29) BVOP utasítása alapján az alábbi

i n t é z k e d é s t

adom ki:

I.

Általános rendelkezések

1. Jelen intézkedés a Kalocsai Fegyház és Börtön (a továbbiakban: Intézet) állományában szolgálatot teljesítő, vagy az Intézethez vezényelt hivatásos szolgálati jogviszonyban, munkavállalói jogviszonyban, rendvédelmi igazgatási szolgálati jogviszonyban, valamint közfoglalkoztatási jogviszonyban álló állománytagokra (a továbbiakban: személyi állomány) terjed ki.
2. Az intézkedés hatálya kiterjed a bv. szervek valamennyi adatkezelésére, amely személyes adatra (ideértve a különleges, genetikai, biometrikus, egészségügyi, bűnügyi személyes adatot stb.) vagy közérdekű, illetve közérdekből nyilvános adatra vonatkozik, az adatkezelés céljától (pl. munkáltatói, gazdasági, bűnüldözési stb.) az adatkezelés típusától (papír alapú, digitálisan kezelt) és az adatkezelési műveletek során alkalmazott eljárástól függetlenül. A bv. szervek területén, illetve területét határoló külső falakon és kapujánál, valamint az elítéltek szállítására szolgáló járműben elhelyezett elektronikus megfigyelési eszközök alkalmazása során jelen utasítás rendelkezései is irányadóak.
3. Az utasítás kibocsátásának célja - a személyes adatok védelméhez fűződő alapvető jogon alapuló információs önrendelkezési jog érvényesülése érdekében - az

adatvédelmi és adatbiztonsági előírások meghatározása, valamint a közérdekű adatok megismeréséhez és terjesztéséhez fűződő alapvető jogon alapuló információszabadság érvényesülése érdekében a bv. szervek kezelésében lévő közérdekű adatok megismerésére irányuló igények elbírálásával, valamint az elektronikus formában közzeendő adatok nyilvánosságra hozatalával összefüggő feladatok meghatározása.

II.

Az Intézet adatvédelmi intézményrendszere, az adatkezelések szintjei

Az adatvédelemre és információszabadságra vonatkozó előírások alkalmazása során adatkezelő szerv vezetőjének kell tekinteni az Intézet parancsnokát.

4. A bv. szerv vezetője felelős:

a) a bv. szerv adatvédelmi és adatbiztonsági intézményrendszerének kiépítéséért és működtetéséért, ennek keretében a személyes adatok védelméhez szükséges személyi, tárgyi és technikai feltételek biztosítását célzó, hatáskörébe tartozó műszaki és szervezési intézkedések megtételéért;

b) az alárendelt személyi állomány adatvédelmi oktatásáért és továbbképzéséért;

c) a bv. szerv tevékenységének rendszeres adatvédelmi ellenőrzéséért, az ellenőrzés során esetlegesen feltárt hiányosságok vagy jogszabálysértő körülmények megszüntetéséért, a személyi felelősség megállapításához szükséges eljárás kezdeményezéséért, illetve lefolytatásáért;

d) a közérdekű adatok megismerhetőségének biztosításáért és az elektronikusan közzeendő közérdekű adatok hozzáférhetővé tételéért;

e) az adatkezeléssel érintettek az Európai Parlament és a Tanács 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 rendeletében (a továbbiakban: általános adatvédelmi rendelet), az információs önrendelkezési jogról és az információszabadságról szóló Info. tv., valamint az adott adatkezelést szabályozó ágazati jogszabályban meghatározott jogainak gyakorolásához szükséges feltételek biztosításáért.

5. A személyi állomány felelős:

a) az utasításban és a bv. szerv adatvédelmi és adatbiztonsági szabályzatában meghatározottak szerint kezeli a feladatai ellátásával összefüggésben tudomására jutott személyes adatokat,

b) betartja az adatkezelésre vonatkozó jogszabályokban, közjogi szervezetszabályozó eszközökben és belső szabályozó eszközökben foglalt előírásokat,

c) tudását naprakészen tartja a feladatellátásra irányadó adatvédelmi és adatbiztonsági előírások kapcsán az adatvédelmi incidensek gyanújának felismerése érdekében.

6. A bv. szerv vezetőjének személyes felelőssége nem zárja ki a személyi állomány érintett tagjának felelősségét.

III.

Harmadik fél bevonás az adatkezelés folyamatába

7. Amennyiben a bv. szerv vezetője döntése alapján valamely feladat ellátása érdekében adatfeldolgozó igénybevétele szükséges, az adatfeldolgozó felelősségét önálló szerződésben vagy a felek között létrejövő szolgáltatási szerződés részeként kell rögzíteni, kivéve, ha az adatfeldolgozó igénybevételének kereteit és garanciális feltételeit jogszabály határozza meg. A szerződés tartalmának összeállítása során ki kell kérni az adatvédelmi tisztviselő véleményét.
8. Amennyiben az érintett bv. szervek vezetője döntése alapján valamely feladat ellátása érdekében közös adatkezelői jogviszony létesítése szükséges, annak részleteit a felek írásbeli megállapodásban rögzítik. A megállapodás tartalmának összeállítása során ki kell kérni az adatvédelmi tisztviselő véleményét.
9. A bv. szervvel szerződéses jogviszonyba kerülő önálló adatkezelővel megkötendő szerződés részeként szükséges rendelkezni a személyes adatok védelme és biztonsága érdekében alkalmazandó intézkedésekről. A szerződés adatkezelést érintő részének összeállítása során ki kell kérni az adatvédelmi tisztviselő véleményét.

IV.

Az Intézet adatvédelmi tisztviselői

10. A bv. szervek vezetői kötelesek az irányításuk alá tartozó személyi állományból az adatvédelmi tevékenység irányítása, felügyelete és ellenőrzése érdekében – a személyes adatok védelmére vonatkozó jogi előírások és jogalkalmazási gyakorlat megfelelő szintű ismeretével rendelkező, a szerv jogszabályokban előírt, személyes adatok kezelésére vonatkozó kötelezettségei teljesítésének elősegítésére alkalmas – adatvédelmi tisztviselőt, valamint akadályoztatása esetére helyettesít, helyetteseket kijelölni. Az adatvédelmi tisztviselő feladatainak gyakorlása során az Intézetparancsnok közvetlen alárendeltségébe tartozik.

Az adatvédelmi tisztviselő részére az Utasítás 15. pontja alapján írásban meg kell határozni a pontos feladatokat. Az adatvédelmi tisztviselő, a feladatai elvégzéséhez szükséges mértékben – a minősített adatra vonatkozó szabályok megtartásával – korlátozás nélkül jogosult a szakterületek adatkezeléseibe, az azzal kapcsolatos ügyiratokba betekinteni.

V.

Az Intézet által vezetett nyilvántartások és a belső adatvédelmi nyilvántartás

11. Az Intézetnek az Utasítás V. fejezetében meghatározott módon kell a nyilvántartásokat vezetnie.

12. A bv. szerv által kezelt, személyes adatot tartalmazó adatkezelések adatvédelmi nyilvántartásba vételét az érintett szakterület az 1. melléklet szerinti adatlap megküldésével kezdeményezi az adatvédelmi tisztviselőnél. A bv. szervek szakterületei gondoskodnak az általuk kezelt személyes adatok vonatkozásában az adatvédelmi adatlap folyamatos felülvizsgálatáról és szükség szerinti aktualizálásáról, az adatvédelmi adatlap tartalmában bekövetkezett változás esetén az aktualizált adatvédelmi adatlapot haladéktalanul továbbítják a bv. szerv adatvédelmi tisztviselője részére.

13. A bv. szervek által kezelt személyes adatokba betekintésekről, valamint az adatok és azok kezelésével összefüggő információk érintett részére való rendelkezésre bocsátásáról az érintett szakterület a 2. melléklet szerinti nyilvántartást vezet, amely tartalmazza:
 - a) betekintést/másolatot kérő, hozzáférési jogot gyakorló nevét, rendelkezésre álló azonosító adatait,
 - b) kérelem keltét,
 - c) igényelt adatok, illetve információk körét,
 - d) kérelem teljesítésének időpontját,
 - e) hozzáférés, betekintés korlátozásának vagy megtagadásának jogi és ténybeli indokait.

14. Az adattovábbításról a 3. melléklet szerinti adattovábbítási nyilvántartást kell vezetni. A nyilvántartás vezetése annak a szakterületnek a feladata, amely az adattovábbítást végezte. A törvényi előíráson alapuló, rendszeres adattovábbításokat elegendő a nyilvántartásban egyszer, a jogszabályi hely megjelölésével, az adattovábbítási időpontok/időszakok megjelölésével, valamint az érintett adatkör és személyi kör megjelölésével feltüntetni, azonban a jogszabályváltozás miatt bekövetkezett változásokat ebben az esetben is dokumentálni kell.

Az adattovábbítási nyilvántartás tartalmazza:

- a) az érintett nevét,
 - b) az adattovábbítás időpontját,
 - c) az adattovábbítás célját és jogalapját,
 - d) az adatigénylő nevét vagy megnevezését,
 - e) a továbbított adatok fajtáját (maguk a szolgáltatott adatok nem képezik az adattovábbítási nyilvántartás részét).
15. Az elutasított közérdekű adatigénylésekről, valamint azok indokairól az Intézet nyilvántartást vezet.

 16. Az Intézethez érkező, adatvédelmi tárgyú, személyes adatra vonatkozó megkeresésekre az ügytípustól függően meghatározott határidőn belül érdemben válaszolni kell, amelyért az Intézetparancsnok-, vagy helyettese által kiszignált személy a felelős. A Hatóság részéről érkezett megkeresést, valamint az elkészített választervezetet az adatvédelmi tisztviselő felterjeszti a BVOP adatvédelmi tisztviselője részére.

17. Az Intézet szakterületei kötelesek a szolgáltatott személyes adatról a személyi állomány tagjára vonatkozóan annak személyi anyaggyűjtőjében, fogvatartott esetében annak fogvatartotti (reintegrációs) anyagában a 3. számú melléklet felhasználásával nyilvántartást vezetni.
18. Az adattovábbítási nyilvántartást az osztályvezetők minden negyedévet követő hónap 13-ig, illetve a IV. negyedévre vonatkozóan december 13-ig megküldik a belső adatvédelmi felelősnek, a Szakutasítás 24. pontjában meghatározott jelentési kötelezettség teljesítéséhez.
19. Bármely jogcímen végrehajtott személyes adat továbbítását külön, önálló csoportszámra kell iktatni. Ezek esetében a tárgymezőben a "személyes adat továbbítása" vagy a "személyes adat továbbításának megtagadása" megjelölés szerepel. Külön csoportszám alkalmazható a személyi állomány és a fogvatartottak személyes adatainak továbbítására.

VI.

A személyes adatok védelme az Intézetnél, az adatkezelés alapvető szabályai

20. Az adatkezelési rendelkezéseket az írott és az elektronikus adatkezelés során egyaránt érvényre kell juttatni. A használaton kívüli, személyes adatokat tartalmazó iratokat és iratgyűjtőket, zárható –, lehetőleg lemez – szekrényben kell elhelyezni. A személyes adatokat tartalmazó papír és elektronikus dokumentumok csak az ügyintézés idejére, a szükséges mértékben kerülhetnek felhasználásra.
20. A személyes vagy különleges adatot tartalmazó papíralapú iratokat, illetve adathordozókat a megismerésre nem jogosult személyek elől elzárva, zárt páncélszekrényben, lemezszekrényben, irodabútorban vagy irattári helyiségben kell őrizni.
21. Személyes adatokat tartalmazó helyiségben az ott szolgálatot teljesítő személyen kívül, - az ellenőrzésre feljogosítottak kivételével - más személy csak az ott szolgálatot teljesítő személy jelenlétében tartózkodhat.
22. Az üresen hagyott, személyes adatokat tartalmazó helyiséget hivatali munkaidő után minden esetben zárva kell tartani, és úgy kell elhagyni, hogy az ott takarítást végző személy adatokhoz ne férhessen hozzá.
23. A személyes adatokat tartalmazó papír, vagy elektronikus dokumentumok felhasználásában érintett helyiségeket, üresen hagyni csak az ajtók zárva tartása mellett lehet.
24. A személyes adatok elektronikus kezelésében érintett helyiségekben a monitorokat úgy kell elhelyezni, hogy a megjelenő adatokat jogosulatlan ne láthassa.
25. A személyes adatokat tartalmazó irattárakat, használaton kívül, az ajtók zárva tartása mellett, pecsétnyomattal ellátott falakattal is le kell zárni.

26. A bűnügyi nyilvántartó csoport, a pénztár, a TÜK, a szerverterem és az informatikai osztály szolgálati helyét biztosító helyiségeket, hivatali munkaidőn kívül, az ajtók zárása mellett, pecsénnyomattal ellátott falakkal is le kell zárni.
27. Az Intézet személyes adatokat tartalmazó helyiségeinek kulcsait, hivatali munkaidőn után, számozott-, pecsénnyomóval ellátott kulcsdobozban, a Biztonsági Osztályra le kell adni.
28. Az egyes helyiségek zárására, a kulcsok tartására és kezelésére vonatkozó helyi rendelkezéseket maradéktalanul be kell tartani.
29. Az informatikai programokat, program-rendszereket, a mindenkori jogszabályok, és országos vagy helyi intézkedések szerint kell használni.
30. Személyes adatot kiadni csak hivatalos írásbeli megkeresés alapján, az adatvédelmi jogszabálynak megfelelően, dokumentáltan engedélyezett.
31. Az irodák takarítását a kijelölt személyi állomány és a fogvatartottak végezhetik. A munkavégzés során a felügyeletet folyamatosan úgy kell biztosítani, hogy az irodában tartózkodó fogvatartott ne ismerhessen meg olyan adatokat, amikre nem jogosult.
32. Az Intézetben elhelyezett FAX készülékek által érkeztetett és továbbított iratokra vonatkozóan az iratkezelési és adatvédelmi szabályokat be kell tartani.
33. A számítógépes rendszerből kezdeményezett nyomtatások eredményét a kezdeményezőnek figyelemmel kell kísérnie, mely nyomtatványért teljes felelősséggel tartozik. A tévesen kinyomtatott adatokat iratmegsemmisítő segítségével kell felismerhetetlenné tenni. Személyes adatokat tartalmazó iratot, nyomtatványt olvasható állapotban tilos a szemébe helyezni.
34. Az Intézet személyes adat átadással járó belső folyamatainak végrehajtásában úgy kell eljárni, hogy az érintettek adatai illetéktelenhez ne kerüljenek.
A Szakutasítás 35. pontjában rögzített, közfoglalkoztatottakkal kapcsolatos szabályok érvényesüléséért az érintett osztály vezetője a felelős.

Személyügyi és Titkársági Osztály

35. A Személyügyi és szervezési osztályon található személyi anyaggyűjtőket és iratokat, arra rendszeresített, zárható lemezszekrényekben kell elhelyezni.
36. A személyi anyaggyűjtők tartalmát és helyét - egyéb intézetparancsnoki utasítás hiányában, - csak az osztály dolgozói módosíthatják.
37. A mindenkori személyügyi programot a személyügyi szakterületen dolgozók hivatalból kezelhetik, abba adatokat vihetnek fel, módosíthatnak vagy törölhetnek.
38. Az Intézet bármely dolgozója - az adatkezelés formájától függetlenül, - jogosult a saját személyi anyagát megtekinteni.

39. A felvételre jelentkező személyes adatait, az osztály dolgozója a jelentkező adatkezelésre vonatkozó hozzájáruló nyilatkozata után kezelheti, és jogosult a felvételi eljárással kapcsolatos minden adatát megismerni.
40. Az ügyirat-kezelési eljárás során a személyes adatokat is tartalmazó dokumentumokat úgy kell kezelni, hogy az abban foglaltakat illetéktelenek ne láthassák.
41. Személyes adatot tartalmazó iratanyagot Intézeten kívülre küldeni lehetőleg a futárszolgálat, vagy intézeti gépjármű igénybevételével kell.
42. Az archív személyi anyagok elhelyezésére külön zárt lemezszekrényt kell használni.
43. A TÜK iroda adatkezelésére az Iratkezelési Szabályzatot kell alkalmazni.

Biztonsági és Fogvatartási Ügyek Osztálya

44. A biztonsági blokkot biztonság-technikával kell védeni, őrizni. Az irodák ajtóinak, zárható szekrényeinek és lemezszekrényeinek kulcsait pecsétlenyomattal ellátott kulcsdobozokban a biztonsági osztály kijelölt helyiségében kell elhelyezni.
45. A kulcsdobozok kiadásakor figyelemmel kell lenni arra, hogy azokat csak a kulcsdobozon feltüntetett személyek vehetik fel. Az egyéb (rendkívüli) esetben történő felnyitás tényét jegyzőkönyv formájában dokumentálni kell.
46. A biztonsági blokkban csak a kijelölt személyi állomány, szolgálati feladat ellátása céljából tartózkodhat, a társosztályok dolgozói - az ellenőrző személyek kivételével - csak szolgálati ügyben léphetnek be.
47. A biztonsági blokk közvetlenül őrzött területének (központi ügyelet, biztonsági tiszt iroda) takarítását fogvatartott nem végezheti.

GEI Informatikai csoport

48. Adatok megismerésére vonatkozó, törvényi felhatalmazással nem rendelkező külső személy, számítástechnikai eszközhöz történő hozzáférése csak titoktartási nyilatkozatot követően, vagy az adatok megismerésének kizártsága esetén engedélyezhető.
49. A számítógépek illetéktelen elindítása elleni védelmet biztosítani kell.
50. Az informatikai csoportvezető felelőssége az informatika rendszerek mentési eljárásainak elkészítése, valamint a mentések végrehajtásának és visszaolvashatóságának ellenőrzése. A napi vezetői értekezletről hangfelvevő eszközzel készített hanganyagot, az intézetparancsnok által meghatározott meghajtón lévő mappában kell tárolni. A mappához való hozzáférést az intézetparancsnok, parancsnok-helyettes és az informatikai csoport tagjai részére lehet kizárólag biztosítani. A hanganyaghoz való hozzáférés célja az Országos Vezetői Értekezletet követően a 30520/661-1/2025.ált. számon kiadott Feladatterv 6. pontjában foglaltak maradéktalan érvényesülésének elősegítése.

51. Az informatikai osztályvezető felelőssége az informatikai rendszer általános hozzáférési szabályainak beállítása, azok kikényszerítése és ellenőrzése.
52. Az informatikai csoport irodáját-, és a szerverterem takarítását kizárólag munkaidőben, az osztály valamely dolgozójának felügyelete mellett szabad végezni.
53. Az adathordozók használata illetve az Intézet területéről történő ki-, bevitele csak az intézetparancsnok, parancsnokhelyettes vagy az informatikai osztályvezető engedélyével történhet.

Egészségügyi és Pszichológiai Osztály

54. Egészségügyi adat továbbítására csak az egészségügyi osztályvezető, főápoló, vagy az általuk kijelölt személy jogosult.
55. Az adatkezelő a tevékenysége során tudomására jutott egészségügyi adatot a munkakörétől, beosztásától függetlenül - orvosi titokként köteles kezelni, illetve megőrizni.
56. Az egészségügyi osztály rendelőiben és egyéb szolgálati helyiségeiben az egészségügyi törzslapot, törzskönyvet, zárójelentést, leletet, egyéb számítógépen vagy kézi módszerrel készített adathordozót (a továbbiakban: egészségügyi nyilvántartást) úgy kell kezelni, illetve tárolni, hogy azokhoz illetéktelen - fogvatartott vagy más jogosulatlan - személy ne férhessen hozzá.
57. Orvosi rendelésen, kezelésen az orvoson és az ápolón kívül más személy csak a fogvatartott hozzájárulásával lehet jelen. Az előállítást szervező döntéshozó biztonsági okok miatt, elrendelheti további biztonsági feladatot ellátó személy jelenlétét, mely esetben az érintett fogvatartott hozzájárulása nélkül is jelen lehet a felügyeletet ellátó személy, aki a tudomására jutott egészségügyi adatot orvosi titokként köteles kezelni.
58. Egészségügyi nyilvántartás, adat intézeten kívülre történő továbbítása biztonságos elektronikus úton (PI: RobotZsarú rendszeren keresztül) vagy kizárólag lezárt borítékban történhet, melyet "Egészségügyi adatok" felirattal kell ellátni.
59. Egészségügyi adatot tartalmazó sérült-, vagy bontott boríték Intézethez érkezése esetén, az esetről az ügykezelő az Iratkezelési Szabályzat előírásai szerint köteles jegyzőkönyvet felvenni. A jegyzőkönyv egy példányát csatolni kell a dokumentumhoz a kézbesítés során.
60. Ha a beteg fogvatartott szállítása, előállítása során állapota rosszabbodására lehet számítani (cukorbetegség, epilepszia miatt stb.), akkor erre a körülményre, a teendő lehetséges intézkedések (elsősegély nyújtás, gyógyszer beadása stb.) megtételére, továbbá az orvosi titok megtartására vonatkozó szabályokra az egészségügyi osztály orvosa, illetve szakápolója köteles felhívni a szállítmányvezető, vagy az előállító biztonsági felügyelő figyelmét, és egyben tájékoztatást adni a speciális helyzetből adódó kötelezettségeiről, jogosultságairól.

Belső ellenőr

61. Az államháztartásról szóló 2011. év CXCV. törvény 70. § (3) bekezdés értelmében a belső ellenőrzést végző személy az ellenőrzött szervnél minősített adatot, üzleti titkot tartalmazó iratokba és más dokumentumokba is betekinhet, azokról másolatot, kivonatot kérhet, személyes adatokat kezelhet az adatvédelmi, illetve a minősített adat védelmére vonatkozó előírások betartásával.

Pszichológus

62. A személyi állomány pszichikai alkalmasság vizsgálata során keletkező dokumentáció orvosi és pszichológusi titoknak, különleges adatnak minősül, így a dokumentációt tartalmazó zárt borítékot kulccsal és pecsétnyomóval lezárt lemezszekrényben kell tárolni.

Műszaki és Ellátási Osztály

63. Az Intézet alaprajzait arra rendszeresített lemezszekrényben kell elhelyezni, azokat kulccsal és pecsétlenyomattal ellátott falakkal is le kell zárni.
64. Az Intézettel szerződésben álló gazdasági társaságok, szervezetek, egyesületek szerződéseit lemezszekrényben kell elhelyezni, azokat kulccsal és pecsétlenyomattal ellátott falakkal is le kell zárni.
65. A munkavállalókhöz kapcsolódó bérjellegű kifizetésekkel (bérpapír, munkába járás elszámolás, napidíj és egyéb költségterítések, cafetéria nyilatkozatok, megrendelők, illetményelőleg megállapodások, különféle analitikák stb.) kapcsolatos iratokat harmadik személy részére kiadni tilos, valamint az ilyen jellegű papírokat minden esetben páncélszekrényben, illetve ennek hiányában zárható szekrényben kell tárolni a felelős őrzés szabályai mellett.
66. A fogvatartottak személyes tárgyait tartalmazó letéti zsákokat minden esetben csak az érintett fogvatartott jelenlétében lehet felnyitni és lezárni. A zárás minden esetben plombával kell, hogy történjen.

Fogvatartási Ügyek Alosztálya

67. Postai küldeményt csak a címzett fogvatartottnak szabad átadni.
68. Munkavégzési időn túl a fogvatartottakra vonatkozó reintegrációs nyilvántartásokat az erre a célra rendszeresített, zárható, lemezszekrényben elzárva kell tárolni, a szekrényeket pecsétlenyomattal is el kell látni.
69. Munkavégzési időn túl a fogvatartottakra vonatkozó bűnügyi nyilvántartásokat az erre a célra rendszeresített zárható lemezszekrényben kell tárolni.
70. A szabadult fogvatartottak nyilvántartásait az erre a célra kijelölt zárható helyiségben kell elhelyezni, és a selejtezésre vonatkozó időtartamig megőrizni.

VII.

Adatkezelések megkezdése, az érintetti jogok

71. Az érintett hozzájárulásán alapuló adatkezelés esetén, az Utasításban meghatározott tájékoztatási kötelezettséget a feladatot végrehajtó személyi állományi tagnak el kell végeznie. A hozzájárulást igazolható módon, elsősorban írásban vagy más rögzített formában kell dokumentálni.
72. Az érintett által benyújtott, hozzáféréshez, helyesbítéshez, az adatkezelés korlátozásához vagy törléshez való joga érvényesítésére irányuló kérelem elbírálása és megválaszolása a bv. szerv a kérelemmel érintett adatkezelést végző szakterületének feladata.

VIII.

Adatvédelmi incidens

73. Adatvédelmi incidens bekövetkezésének észlelése esetén haladéktalanul jelentést kell tenni a bv. szerv szakterületi vezetőjének. A szakterület vezetője haladéktalanul értesíti az adatvédelmi tisztviselőt az adatvédelmi incidens bekövetkezéséről és rendelkezésére bocsátja az incidenssel kapcsolatban rendelkezésre álló iratokat és információkat, amennyiben az előzetes felmérés alapján valószínűsíthetően kockázattal jár az adatvédelmi incidens. Amennyiben a felmérés során megállapítja, hogy nem jár kockázattal az incidens, írásban tájékoztatja az adatvédelmi tisztviselőt az adatvédelmi incidens bekövetkezéséről.
74. Az adatvédelmi tisztviselő a rendelkezésre álló iratok, információk alapján, valamint szükség esetén az érintett szakterület(ek), illetve a szükséges szakértelemmel rendelkező személy bevonásával elvégzi a kockázatbecslést a bekövetkezett adatvédelmi incidenssel összefüggésben, majd az eredménytől függően elvégzi az Utasítás VIII. fejezetének 47.-48. pontjában meghatározott feladatokat.

A bv. szervek az általuk kezelt adatokkal összefüggésben felmerült adatvédelmi incidensekről a 4. melléklet szerinti jegyzőkönyvekből álló nyilvántartást vezetnek, mely tartalmazza az incidens

- a) leírását, bekövetkezésének körülményeit (helye, időpontja, oka stb.),
- b) hatásait (érintetti jogok sérülése, érintetti kör nagysága stb.),
- c) kezelésére tett intézkedéseket (kezelés módja, időpontja, Hatóságnál való bejelentés, érintett értesítése esetén ennek ténye stb.).

IX.

Adatbiztonsági intézkedések

75. A személyes adatok fizikai biztonságának biztosítása érdekében az adatkezelések során a személyes vagy különleges adatot tartalmazó papír alapú iratokat, illetve adathordozókat páncélszekrényben vagy biztonsági zárral és szárazlakattal ellátott

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

76. A személyes adatok megfelelő szintű biztonságának biztosítása érdekében az egyes adatkezelésekhez a hozzáférési jogosultságot a jogosult eljárójának személyre szólóan kell megállapítani, figyelemmel a kijelölt vagy felhatalmazott személy beosztására és az ahhoz kapcsolódó jogszabályban meghatározott feladatra. A jogosultságot az érintett munkaköri leírásában is rögzíteni kell. Amennyiben a jogosultság megállapítására alapot adó körülményben változás történik, haladéktalanul intézkedni kell a jogosultság módosítására vagy visszavonására.
77. A jogosultságot megállapító vezető köteles gondoskodni arról, hogy a betekintési és hozzáférési jogosultságok a személyzeti változásokkal összhangban aktualizálásra kerüljenek. A személyi állomány tagja jogviszonyának megszűnése esetén legkésőbb az érintett utolsó munkában töltött napján intézkedni kell a betekintési és hozzáférési jogosultságok visszavonására. A leszerelő lap mindaddig nem írható alá, amíg a betekintési, illetve hozzáférési jogosultság visszavonásának tényét a leszerelő lap szignálásával az arra hatáskörrel rendelkező szakterületek nem igazolták.

X.

A közérdekű adatok közzétételének és a közérdekű adatigénylések intézésének eljárási szabályai

78. A közérdekű adatigénylés teljesítésére az igény beérkezésétől számított legfeljebb 15 nap áll rendelkezésre, a határidő a bv. szervhez érkezést követő munkanapon kezdődik. Az adatvédelmi tisztviselő az adatigénylés beérkezését követően haladéktalanul megvizsgálja az adatigénylést. Amennyiben az adatigénylés nem egyértelmű, a bv. szerv felhívja az adatigénylőt az igény pontosítására. Ha az adatigényléssel érintett adat elektronikus formában nyilvánosan elérhető, az adatigénylés teljesíthető az adatot tartalmazó nyilvános forrás megjelölésével is.
79. Az adatvédelmi tisztviselő megvizsgálja, hogy az igénylő nyújtott-e be azonos adatkörre vonatkozó adatigénylést. Amennyiben megállapításra kerül, hogy az igényelt adatok megegyeznek az azonos igénylő által egy éven belül benyújtott adatigénylésben szereplő adatokkal, a bv. szerv nem köteles eleget tenni az adatigénylésnek abban a részében, feltéve, hogy az azonos adatkörbe tartozó adatokban változás nem állt be. Ennek érdekében a bv. szervek gondoskodnak az egy éven belül benyújtott közérdekű adatigényléseknek visszakereshetőségéről.
80. Ha az adatigénylés jelentős terjedelmű, illetve nagyszámú adatra vonatkozik, vagy az adatigénylés teljesítése a bv. szerv alaptervekenységének ellátásához szükséges munkaerőforrás aránytalan mértékű igénybevételével jár, az adatigénylés teljesítésére rendelkezésre álló 15 napos határidő egy alkalommal 15 nappal meghosszabbítható, erről a bv. szerv az adatigénylőt az igény beérkezését követő 15 napon belül tájékoztatja.

XI.

Ellenőrzés

81. Az adatkezelési rendelkezések betartásának ellenőrzésére az Utasítás 96. pontjában felsorolt személyek jogosultak. Az ellenőrzésre feljogosított az ellenőrzés céljára figyelemmel az ellenőrzés érdekében minden olyan helyiségbe beléphet, ahol adatkezelés folyik, az adatkezelést végzőktől minden olyan kérdésben felvilágosítást kérhet, minden olyan adatkezelést megismerhet, vagy abba betekinthet, amely az ellenőrzött bv. szerv adatkezelési tevékenységével összefügg, és az adatok megismerését jogszabály nem korlátozza.

XII.

Oktatás, tájékoztatás

82. A bv. szerv állományába újonnan felvételre került személyek adatvédelmi oktatása a központi elektronikus képzési rendszerben kerül végrehajtásra. A bv. szerv állományába újonnan felvételre került személyeket a munkakörből fakadó sajátosságokra tekintettel, indokolt esetben az adatvédelmi tisztviselő kiegészítő adatvédelmi oktatásban részesíti, amelynek keretében a szükséges jogszabályokat, belső szabályozó eszközöket és egyéb segédanyagokat rendelkezésre bocsátja. Az adatvédelmi tisztviselő a bv. szerv személyi állományát a személyes és közérdekű adatok kezelését érintő jogszabály- és egyéb normaváltozásokról köteles tájékoztatni, indokolt esetben – különösen a jelentősebb változások vagy az ellenőrzés során feltárt visszatérő vagy egyébként súlyos hiányosságok esetén – az érintett állomány kötelező adatvédelmi oktatását elvégezni.
83. Az adatvédelmi tisztviselő az adatkezelő szerv személyes adatok kezelését végző személyi állományát a bekövetkezett adatvédelmi tárgyú jogszabály- és normaváltozásokról köteles tájékoztatni, indokolt esetben – különösen a jelentősebb adatvédelmi tárgyú normaváltozások vagy az ellenőrzés során feltárt visszatérő vagy egyébként súlyos hiányosságok esetén – az érintett állomány kötelező adatvédelmi oktatását elvégezni.
84. Az adatvédelmi tisztviselők rendszeres továbbképzéséről a BVOP adatvédelmi tisztviselője gondoskodik.

XII.

Záró rendelkezések

85. Jelen intézkedésem a kiadás napján lép hatályba, ezzel egyidejűleg veszti a **30520-0/377/2026. int.** számú intézetparancsnoki intézkedés.

**Vajda Szabolcs bv. alezredes
parancsnok**

Készítette: Sárdi Gábor bv. alezredes
Készült: 1 eredeti példányban
Kapja: TÚK
Elérhetőség: elektronikusan az intézetparancsnoki intézkedések között

Mellékletek:

1. sz.melléklet: Adatlap adatvédelmi nyilvántartásba vételhez

2. sz.melléklet: Betekintési nyilvántartás
3. sz.melléklet: Adattovábbítási nyilvántartás
4. sz.melléklet: Jegyzőkönyv adatvédelmi incidensről
5. sz.melléklet: Bv. szervek által közzéteendő közadatok listája

ZÁRADÉK

A dokumentum elektronikus aláírással hitelesített
30520/377-2/2026.ált