A VÁCI FEGYHÁZ ÉS BÖRTÖN PARANCSNOKÁNAK
98/2021. számú
I N T É Z K E D É S E

Vác, 2021. november 4.

A Váci Fegyház és Börtön Adatvédelméről és Adatbiztonsági Szabályzatáról

Az információs önrendelkezési jogról és az információs szabadságról szóló 2011. évi CXII. törvény 25/A. § (3) bekezdés, valamint a büntetés-végrehajtási szervezek Adatvédelmi és Adatbiztonsági Szabályzatáról szóló 3/2019. (III. 20.) utasítás 5., és 84. pontja rendelkezéseire figyelemmel, az alábbi

i n t é z k e d é s t

adom ki:

I. ÁLTALÁNOS RENDELKEZÉSEK

1. Jelen intézkedés célja, hogy a Váci Fegyház és Börtön (továbbiakban: Intézet) tevékenysége során a személyes adatok védelméhez fűződő alkotmányos alapjogon alapuló információs önrendelkezési jog érvényesülésének biztosítására, illetve az Intézet által kezelt személyes adatok jogosulatlan felhasználása megakadályozásának érdekében meghatározza a személyes adatok kezelése során irányadó adatvédelmi és adatbiztonsági előírásokat.

2. Jelen intézkedés a büntetés-végrehajtási szervezek Adatvédelmi és Adatbiztonsági Szabályzatáról szóló 3/2019. (III. 20.) utasítással (a továbbiakban: Utasítás), valamint a személyes adatok védelmére vonatkozó jogszabályokkal együtt alkalmazandó.

3. A személyes adat fogalma tágan értelmezendő, így személyes adatnak minősül minden olyan információ, ami az adott, azonosított vagy azonosítható személyt jellemzi, rá vonatkozik, vagy vele kapcsolatba hozható, továbbá mindazon információk, amelyek összegyűjtése egy bizonyos személy azonosításához vezethet; így különösen az iraton, kép- és hangfelvételen szereplő adatok, a szóban elhangzó információk, bármiféle információ vagy ismeret.

4. Az érintett személyes adatainak kezelése, így különösen az adatok rögzítése, megismerése, azokról másolat készítése, törlése illetve az adattovábbítás tekintetében - az adatkezelés jogalapjától függően - a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről szóló Európai Parlament és Tanács 2016/679. (2016. április 27.) rendelet (általános adatvédelmi rendelet; a továbbiakban: Adatvédelmi Rendelet), illetve jogszabály, így különösen az információs önrendelkezési jogról és az információs szabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Info. tv.), a rendvédelmi feladatokat ellátó szervek hivatásos állományának szolgálati jogviszonyáról szóló 2015. évi XLII. törvény, a munka törvénykönyvéről szóló 2012. évi I. törvény, a büntetések, az intézkedések, egyes kényszerintézkedések és a szabálysértési elzárás végrehajtásáról szóló 2013. évi CCXL. törvény (a továbbiakban: Bv. tv.), a büntetés-végrehajtási szervezetről szóló 1995. évi CVII. törvény (a továbbiakban: Bvsz. tv.), az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény, az egészségügyről szóló 1997. évi CLIV. tv. rendelkezései irányadók.

5. Jelen intézkedés - a foglalkoztatási jogviszonyra, vagy szerződéses jogviszonyra tekintet nélkül - azon munkatársakra (a továbbiakban: adatkezelést végző személyi állományi tagok) vonatkozik, akik:

a) az intézet számítógépes adatállományaihoz, elektronikus információs rendszerekhez (a továbbiakban: adatok) bármilyen célból hozzáférhetnek, így akik napi munkájuk során használják ezeket az adatokat és azok is, akik alkalmilag, vagy rendszeresen kezelik azokat.
b) személyes adatokat tartalmazó papír alapú iratokat, vagy más adathordozót (a továbbiakban: okirat) kezelnek.

6. Az adatkezelést végző személyi állományi tagok a feladatvégzésük során a munkaköri leírásban, vagy más, rájuk vonatkozó meghatározásban (pl. szerződés) rögzítettek szerint, a jogszabályok és a Szabályzat keretei között kezelik az adatokat, betartva az ügyrendi előírásokat (pl. ki módosíthat adatot, mely adatot módosíthat), valamint a számítógépek kezelésére vonatkozó szabályokat, az adatok logikai vagy fizikai sérülésének elkerülése érdekében.

7. Az adatkezelést végző személyi állományi tagok az adatokat a munkakörükhöz kapcsolódóan, illetve a számukra meghatározott feladat (a továbbiakban: munkakör) végrehajtása során kezelik, azokat egyéb módon nem használhatják, különösen indokolatlanul, felhatalmazás nélkül:

a) az adatokról nem készíthetnek másolatot, kivéve az előírt biztonsági mentéseket,
b) az adatokat nem nyomtathatják ki, azok a nyomtatás után nem maradhatnak felügyelet nélkül,
c) az adatokat nem küldhetik el e-mailben,
d) az adatokhoz nem engedhetnek illetéktelen hozzáférést sem közvetlenül a számítógépnél, sem hálózaton vagy interneten keresztül, vagy okirat formájában,
e) az adathordozókat nem vihetik ki a bv. szerv területéről.

8. A számítógépes alrendszerek adattartalmához való hozzáférés (jogosultsági szintek betartásával) az adatkezelést végző személyi állományi tagok számára szakaszoltan, a munkakörhöz igazodó mértékben, a szervezeti egységek vezetőinek írásbeli meghatározása alapján biztosítandó.

9. Az adatokat (pl. szövegszerkesztővel és táblázatkezelővel írt dokumentumok) az adatkezelést végző személyi állományi tagok az előírt helyre mentik, annak érdekében, hogy az adat a biztonsági mentésbe bekerüljön; az ideiglenes munka állományok törlésére a végleges anyag elkészültekor intézkedik.

10. Ideiglenes adatmásolatokat, próbanyomtatásokat, elrontott nyomtatásokat a munka végeztével az adatkezelést végző személyi állományi tagok megsemmisítik, annak érdekében, hogy adat illetéktelenek számára ne legyen kinyerhető.

11. Az adatok sérüléséről, annak lehetőségéről vagy illetéktelenhez jutásáról való tudomásszerzés esetén a kijelölt személyt (rendszergazda és adatvédelmi tisztviselő) az adatkezelést végző személyi állományi tagok tájékoztatják.

12. Az informatikai jogosultság és hozzáférési környezetet oly módon kell létrehozni, hogy az informatikai rendszer alkalmas legyen a kezelt adathoz történő hozzáférés korlátozására, ennek értelmében az adatok illetéktelen harmadik személytől védettek.

II. AZ ADATKEZELŐ SZERV VEZETŐJÉNEK FELELŐSSÉGE, FELADAT- ÉS HATÁSKÖRE

13 Az Intézet adatkezelésének törvényességéért az intézetparancsnok felelős, akinek felelősségi körét és feladatait az Utasítás 5. és 8. pontjai tartalmazzák.

14. Az Intézet szervezeti egységei adatkezelésének törvényességéért illetékességi területükön a szakterületi vezetők felelősek. A vezetői felelősség nem zárja ki a jogsértést ténylegesen elkövető személyi állományi tagok felelősségét.

III. AZ INTÉZET ADATVÉDELMI TISZTVISELŐJE

15.Az Intézet adatkezelésének törvényessége érdekében az intézetparancsnok adatvédelmi tisztviselőt, valamint akadályoztatása esetére helyettest jelöl ki.

16Az adatvédelmi tisztviselő feladat- és hatáskörét az Utasítás 15. pontja részletezi.

17. Az adatvédelmi tisztviselő adatvédelemmel összefüggő feladatainak ellátása során szükség szerint együttműködik az informatikai szakterülettel és az elektronikus információs rendszer biztonságáért felelős személlyel, valamint az adatkezeléssel érintett szakterületekkel.

IV. NYILVÁNTARTÁSOK VEZETÉSE ÉS AZ ADATVÉDELMI NYILVÁNTARTÁS

1. Az adatkezelésre vonatkozó nyilvántartások

18. Az adatvédelmi nyilvántartásba vételt a szakterületek az Utasítás 1. mellékletének az adatvédelmi tisztviselő részére történő megküldésével kezdeményezik.

19. A szakterületek gondoskodnak az adatvédelmi adatlap folyamatos aktualizált állapotáról, változás esetén az adatvédelmi tisztviselő részére átadják az adatvédelmi adatlapot.

20. A szakterületek az Utasítás 2. melléklete alapján irat betekintési nyilvántartást kötelesek vezetni.

21. Az adattovábbításról és adatszolgáltatásról adattovábbítási nyilvántartást kell vezetni az Utasítás 3. melléklete alapján. A rendszeres adattovábbításokat az Utasítás 21. pontjában foglaltaknak megfelelően kell feltüntetni az adattovábbítási nyilvántartásban. Az adattovábbítási nyilvántartás vezetése minden szakterület számára kötelező, aki adattovábbítást teljesít.

22. A szakterületek kötelesek haladéktalanul az adatvédelmi tisztviselőt tájékoztatni a beérkezett közérdekű adatigénylés vonatkozásában.

23. Az elutasított közérdekű adatigénylésről a szakterületek kötelesek haladéktalanul az adatvédelmi tisztviselőt tájékoztatni.

2. Adathordozókra vonatkozó védelmi intézkedések

24. Az adathordozókat a hagyományos adathordozókra vonatkozó ügyiratkezelési szabályok szerint minősíteni kell a tárolt adat alapján, azt az adathordozó címkéjén fel kell tüntetni.

25. Az adathordózók használata, illetve intézet területéről történő kivitele/behozatala az intézetparancsnok engedélyével történhet.

3. Szakterületek feladatai

3.1 Személyügyi és Titkársági Osztály

26. A személyes adatok védelme érdekében a Személyügyi és Titkársági Osztályon található személyi anyaggyűjtőket és iratokat, arra rendszeresített lemezszekrényekben kell elhelyezni, azokat kulccsal és pecsétlenyomattal ellátott falakattal is le kell zárni, a kulcsokat az iroda számozott kulcsdobozában a személykapun le kell adni.

27. A személyügyi programot csak a személyügyi szakterületen dolgozó adatkezelést végző személyi állományi tagok kezelhetik, minden dolgozó jogosult a saját elektronikus személyi anyagát megtekinteni. Betekintési, lekérdezési jogosultsággal rendelkezik az intézet parancsnoka és helyettese, valamint a fegyelmi és nyomozó tiszt.

28. A Robotzsaru integrált ügyviteli rendszert illetően további adatkezelési (pl.: éves rendes, tanulmányi vagy egészségügyi szabadságot illetően) és lekérdezési jogosultsággal rendelkezők körét vezetői döntés alapján az ügykezelési csoport kijelölt tagja kezeli, és szükség esetén gondoskodik a módosításokról.

29. A személyügyi alapnyilvántartásba és az annak alapjául szolgáló iratokba csak a rendvédelmi feladatokat ellátó szervek hivatásos állományának szolgálati jogviszonyáról szóló 2015. évi XLII. törvény (továbbiakban: Hszt. 275. §-ában meghatározott személyek tekinthetnek be.)

30. A személyügyi nyilvántartás adatkörét a Hszt. 1. melléklete határozza meg.

31. A személyi anyaggyűjtőbe dokumentumot elhelyezni, onnan kivenni vagy arról másolatot készíteni csak és kizárólag a személyügyi szakterület adatkezelést végző személyi állományi tag végezhet a vonatkozó jogszabályok alapján.

32. A dolgozó munkaviszonyával kapcsolatos és bemutatott iratokat, illetve azokról készített, és az eredetivel megegyező másolatot a személyügyi szakterület adatkezelést végző személyi állományi tagjai helyezik el a személyi anyaggyűjtőbe, viszik fel a személyügyi programba.

33. Felvételre jelentkezők esetében a jelentkezők nyilatkoznak a személyes adataik kezelhetőségéről, sikertelen felvétel esetén az adatkezelést végző személyi állományi tagok az adatokat a nyilatkozatban meghatározott határidővel megsemmisítik, melyről jegyzőkönyvet készítenek.

34. A felvételi eljárás során az adatkezelést végző személyi állományi tagok jogosultak megismerni a jelentkező fizikai állapotfelmérés adatait, továbbá az egészségügyi, pszichikai és kifogástalan életvitel vizsgálat eredményeit.

35. Dolgozó áthelyezése esetén az iratanyag megküldése futárszolgálat, illetve intézeti gépjármű igénybevételével, az elektronikus adattovábbítás Szenyor for Windows rendszerben történhet.

36. Az archív anyagok elhelyezésére külön zárt lemezszekrényt szükséges alkalmazni, amelyet zárható helységben kell kulccsal és pecsétlenyomattal ellátott falakattal lezárva tárolni, tételes nyilvántartás mellett.

37.Személyes adat kiadása csak hivatalos írásbeli megkeresés alapján, az adatvédelmi jogszabálynak megfelelően, dokumentálva engedélyezett.

38. A TÜK iroda adatkezelésére az Iratkezelési Szabályzatot megfelelően alkalmazni kell.

3.2. Biztonsági Osztály

39. A biztonsági blokkot biztonság-technikával kell védeni, őrizni, a hivatali munkarendben használt irodák ajtóit zárni kell a munkaidő végén, kulcsait kulcsdobozban a biztonsági osztályon kell elhelyezni, vagy a személykapun tárolni.

40. A biztonsági blokkban csak a kijelölt személyi állomány, szolgálati feladat ellátása céljából tartózkodhat.

41. A biztonsági blokk közvetlenül őrzött területének (központi ügyelet, biztonsági tiszti iroda) takarítását fogvatartottak fokozott biztosítás mellett végezhetik. A fegyverszoba, szakanyag raktár takarításában fogvatartott nem vehet részt! Az egyéb irodák takarítását a kijelölt személyi állomány és a fogvatartottak végezhetik. A munkavégzés során a felügyeletet folyamatosan biztosítani kell, kiemelt figyelmet kell arra fordítani, hogy az irodában tartózkodó fogvatartott ne ismerhessen meg olyan adatokat, amikre nem jogosult.

42. Munkavégzési időn túl, valamint használaton kívül a fenti adatokat tartalmazó dokumentumokat, nyilvántartásokat zárható lemezszekrényben, páncélszekrényben, valamint egyéb zárható iratszekrényben, fiókban kell tárolni.

3.3. Informatikai Osztály

43. A számítógép illetéktelen elindítása elleni védelmet biztosítani kell. A vonatkozó részletszabályokat az Iratkezelési Szabályzat, az Informatikai Biztonsági Szabályzat, valamint az Informatikai Biztonsági Kézikönyv határozza meg.

44. Az adatmegőrzés érdekében folyamatosan biztosítani kell, hogy az adathordozó az adott technikai feltételek mellett olvasható maradjon, vagy olvasható állapotba kerüljön.

45. Az Intézet folytonos működésének fenntartásához biztosítani kell a feldolgozott adatállományok reprodukálhatóságát az informatikai adatok Iratkezelési szabályzatában és „az intézeti informatikai, számítástechnikai tevékenység szabályozása” tárgyú intézetparancsnoki intézkedésben meghatározott időszakonkénti mentésével. A mentések szakszerű végrehajtásáért, tárolásáért, ellenőrzéséért az informatikai osztályvezető felelős. Az elkészített mentéseket az Iratkezelési Szabályzatban meghatározott időszakonként ellenőrizni kell az adatok visszaállíthatósága szempontjából. Az ellenőrzéseket az informatikai szakterület dokumentáltan végzi.

46. Az intézetben használt informatikai rendszereket illetően a hozzáférési jogosultságokról az informatikai osztályon pontos és naprakész nyilvántartást kell vezetni, amelynek felelőse az informatikai osztályvezető.

47. Az informatikai osztályvezető végezze el az adatbázisokhoz, nyilvántartásokhoz való hozzáférések ellenőrzését a szakterületi vezetők bevonásával. Ilyen tárgyú ellenőrzést évente ismételten el kell végeznie.

48. A szerverek védelme érdekében az erre kijelölt személyi állomány tagja az Informatikai Osztály ajtóit biztonsági hevederzárral zárja le, kulcsait kulcsdobozban a személykapun adja le minden esetben.

49. A kulcsdobozt csak az Informatikai Osztály dolgozói vehetik fel, a rendkívüli esetben történő felnyitás tényét a meghatározottak szerint dokumentálni kell.

50. Más szakterületek dolgozói gépterembe történő belépése és ott-tartózkodása csak az Informatikai Osztály dolgozóinak jelenlétében engedélyezett.

51. A gépterem takarítását kizárólag munkaidőben, az Informatikai Osztály dolgozójának felügyelete mellett szabad végezni.

3.4. Egészségügyi Osztály

52. Az egészségügyi és személyazonosító adatok kezelése során biztosítani kell az adatok biztonságát vétlen vagy szándékos megsemmisítéssel, megsemmisüléssel, megváltoztatással, károsodással, nyilvánosságra kerüléssel szemben, továbbá, hogy azokhoz illetéktelen személy ne férjen hozzá.

53. Egészségügyi adat továbbítására jogosultak a munkakörünél fogva adattovábbításra jogosult adatkezelést végző személyi állományi tagok.

54. Az egészségügyi adatok védelmének felelőse az egészségügyi osztály vezetője.

55. A betegellátó a tevékenysége során tudomására jutott egészségügyi adatot a munkakörétől, beosztásától függetlenül - orvosi titokként köteles kezelni, illetve megőrizni.

56. Az adatkezelő mentesül a titoktartási kötelezettség alól, egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény 7. § (2) bekezdésében foglaltak alapján.

57. 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.

58. Az egészségügyi dokumentációkat biztonságosan zárható tárolókban kell tartani, a tárolóeszközök kulcsait csak az adatkezelésre jogosult személyi állományi tagok jogosultak kezelni.

59. Az orvosi vizsgálaton a bv. orvos, és az egészségügyi személyzet (ide értve a nem bv. alkalmazásban álló egészségügyi dolgozókat is) lehet jelen. Indokolt esetben a vizsgálat során jelen lehet a fogvatartottal azonos nemű, biztonsági feladatokat ellátó személy is, aki a tudomására jutott egészségügyi adatokat az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvényben foglaltaknak megfelelően köteles orvosi titokként kezelni.

60. A FŐNIX egészségügyi modul alkalmazása során a 64/2020. (XII.12.) BVOP utasítás alapján kell eljárni.

61. Egészségügyi nyilvántartás, adat intézeten kívülre történő továbbítása kizárólag lezárt borítékban történhet. A borítékot "Egészségügyi adatok" felirattal kell ellátni.

62. Ha az egészségügyi adatokat tartalmazó postai úton érkezett dokumentum sérült vagy bontott, az esetről az ügykezelő az Iratkezelési Szabályzat előírásai szerint köteles jegyzőkönyvet felvenni. A jegyzőkönyv egy példányát csatolni kell a dokumentum a kézbesítése során.

63. Amennyiben a fogvatartott egészségügyi ellátása indokoltan a váci Jávorszky Ödön Városi Kórházban történik, az ellátást végző orvos kérésére az intézet orvosa vagy szakápolója bocsássa rendelkezésére a betegről kért egészségügyi nyilvántartásokat.

64. Az előző pontban foglaltak alapján kell eljárni abban az esetben is, ha az egészségügyi ellátást a városi ügyeletes orvos, vagy a mentőszolgálat orvosa végzi.

65. Ha a beteg fogvatartott szállítása, előállítása során állapota rosszabbodására lehet számítani (cukorbetegség, epilepszia miatt stb.), akkor erre a körülményre, a teendő lehetséges intézkedések (elsősegélynyújtás, gyógyszer beadása stb.) megtételére, továbbá az orvosi titok megtartására vonatkozó szabályokra az egészségügyi osztály orvosa, illetve szakápolója hívja fel a szállítmányvezető, vagy az előállító biztonsági felügyelő figyelmét, és egyben tájékoztatást adjon a speciális helyzetből adódó kötelezettségeiről, jogosultságairól.

66. A beteg fogvatartott állapota rosszabbodásának lehetőségét az átadás-átvételi elismervényre, illetve az előállítási rendelvényre, rendelkezésre az Egészségügyi Osztály beosztottja vezeti rá.

3.5. Belső ellenőr

67. A belső ellenőrzést végző személy az államháztartásról szóló 2011. évi CXCV. törvény 70. § (3) bekezdése, valamint a költségvetési szervek belső kontrollrendszeréről és belső ellenőrzéséről szóló 370/2011. (XII.31.) kormányrendelet (továbbiakban: Bkr.) 22. § (2) b) és f), a 25. § b), valamint a 26. § h), j) és k) pontjai alapján tekinthet be iratokba és dokumentumokba, kezelhet személyes adatokat az intézetnél.

68. Külső szolgáltató belső ellenőrzési tevékenységbe történő bevonása esetén a Bkr. 16. § (3) bekezdés szerint kell eljárni.

69. Lezárt belső ellenőri jelentés nyilvánosságra hozása esetén a Bkr. 44. § (3) bekezdés rendelkezései az irányadók.

3.6. Pszichológus

70. A személyi és a fogvatartotti 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 szükséges tárolni. A vizsgálati anyagot tartalmazó borítékon rögzíteni kell, hogy azt csak orvos, vagy szakpszichológus bonthatja fel.

71. A pszichikai alkalmasságot vizsgáló eljárások során az adatok felvételét, rögzítését a szakpszichológus és a pszichológus egyaránt végezheti, a vizsgálati eredmények pszichológusi titokként való kezelése mellett.

72. A személyi állomány mentálhigiénés gondozása során a szakterület dolgozója a tudomására jutott személyes adatokat a pszichológusok szakmai etikai kódexében rögzített szakmai elvek szerint köteles kezelni.

73. A fogvatartotti állomány pszichés ellátásának adminisztrációja során a szakterület dolgozója véleményét a pszichológusi szakma etikai elveinek figyelembe vételével fogalmazza meg oly módon, hogy a fogvatartottról készített vélemény lehetőség szerint a pszichológusi titkok megtartása mellett segítse a büntetés-végrehajtás céljainak megvalósítását.

3.7. Gazdasági Osztály

74. A személyes adatok védelme érdekében a gazdasági osztályon található személyes adatokat tartalmazó iratokat, a személyi állományi tagok az arra rendszeresített

lemezszekrénybe helyezzék el, azokat negatív pecsétlenyomóval lássák el, illetve kulccsal zárják le, a kulcsokat az iroda számozott kulcsdobozában a személykapun adják le.

75. Az intézet alaprajzait, az intézettel szerződésben álló Kft-k, szervezetek, egyesületek szerződéseit arra rendszeresített lemezszekrényben kell elhelyezni, azokat kulccsal le kell zárni.

76. A dolgozók részére rendszeresített ruházatról, munka- és védőruháról, vegyvédelmi eszközökről vezetett könyveket, kartonokat zárható szekrényben szükséges tartani.

77. A szolgálati gépjárművekhez rendszeresített üzemanyag kártyák zárt szekrényben egy páncélkazettában tarthatók. Az üzemanyag kártyákhoz tartozó PIN kódokat a gazdasági osztályvezető-helyettes (fogvatartási) lezárt szekrényben tárolja.

78. Fogvatartotti munkáltatási helyeken a fogvatartottak adatait tartalmazó iratokat (munkaidő nyilvántartás, fogvatartotti karton) elzártan kell tárolni.

79. A fogvatartottak munkáltatásával kapcsolatos adatok, nyilvántartások, dokumentumok (munkáltatási könyv, munkahely, munkadíj besorolás, munkadíj- és ösztöndíj elszámolás) tárolása csak elzárt helyen történhet.

80. Munkavégzési időn túl a személyi állomány és fogvatartottak adatait tartalmazó iratokat, baleseti és egyéb jegyzőkönyveket, oktatási anyagokat, minden hivatalos iratot a páncélszekrényben kell elhelyezni.

81. A pénzkezelési szabályzatban meghatározottak alapján a pénztárba történő belépés, csak az engedélyezett személyek számára lehetséges.

82. A pénztárban tartott pénzösszeget, utalványokat, pénzhelyettesítő fizetési eszközöket a meghatározottak alapján biztonsági zárral ellátott páncélszekrényben kell tárolni, melyet 2 db kulccsal és pecsétlenyomattal ellátott falakattal kell lezárni.

83. A munkavállalókhoz kapcsolódó bérjellegű kifizetésekkel (bérpapír, munkába járás elszámolás, napidíj és egyéb költségtérítések, cafetéria nyilatkozatok, megrendelők, illetményelőleg megállapodások, különféle analitikák stb.) kapcsolatos iratokat harmadik személy részére kiadni tilos, valamint az ilyen jellegű adathordozókat minden esetben páncélszekrényben, illetve ennek hiányában zárható lemezszekrényben kell tárolni a felelős őrzés szabályai mellett.

84. Az intézet pénzkészletét tartalmazó kivonatokat zárható szekrényben kell tárolni.

85. A kötelezettségvállalásról szóló szabályzatban meghatározottak alapján történhetnek az intézetet érintő kiadások, illetve bevételek aláírásai, igazolásai.

86. Az utalások végrehajtására csak és kizárólag az jogosult, aki az utaláshoz szükséges PIN kóddal ellátott kártyával rendelkezik, valamint a kötelezettségvállalási szabályzatban felhatalmazást kapott. Az utaláshoz szükséges kártyákat minden esetben zárható páncélszekrényben kell tárolni.

87. A KGR FORRÁS SQL programban rögzített zárt bizonylatokat csak az erre jogosult személy nyithatja vissza.

88. A fogvatartottak egyéni felszerelési termékeinek nyilvántartására szolgáló kartonok, valamint a szállítással - befogadással kapcsolatos nyilvántartásokat elzárt helyen kell tárolni.

89. Fogvatartottak adatait tartalmazó dokumentumok (letiltási rendelvények, kártérítési határozatok, kérelmi lapok, kiétkezési, telefonálási listák) tárolása zárt szekrényben történik.

3.8. Büntetés-végrehajtási Osztály

90. A fogvatartottak részére érkező iratok kézbesítése során kiemelt figyelemmel kell eljárni tekintettel arra, hogy névazonosság esetén jogszabálysértés fordulhat elő. A fogvatartottnak személyesen kell átadni a küldeményt. Tilos zárkatársnak átadni, vagy üres zárkában hagyni postai küldeményt!

91. Munkavégzési időn túl a fogvatartottakra vonatkozó reintegrációs, valamint a bűnügyi nyilvántartásokat az erre a célra rendszeresített, zárható, lemezszekrényben elzárva kell tárolni, a szekrényeket pecsétlenyomattal is el kell látni.

92. A szabadult fogvatartottak nyilvántartásait az erre a célra kijelölt zárható helyiségben, kategorizálva kell elhelyezni, és a selejtezésre vonatkozó időtartamig megőrizni.

V. ADATVÉDELMI HATÁSVIZSGÁLAT ÉS ELŐZETES KONZULTÁCIÓ

93. Valamennyi új, vagy korábbiaktól eltérő adatkezelést előíró vagy eredményező jogszabály vagy belső szabályozó eszköz, eljárásrend vagy technológia bevezetését vagy változását megelőzően, az előkészítés során az adatvédelmi tisztviselő megvizsgálja, hogy a tervezett adatkezelésnek várhatóan milyen hatásai lesznek az érintettek alapvető jogai érvényesülésére (a továbbiakban: előzetes kockázatbecslés).

94. Az Utasítás 26. pontjában foglalt esetekben az adatvédelmi tisztviselő az érintett szakterületek bevonásával írásban előzetes kockázatbecslést készít.

95. A hatásvizsgálat lefolytatása esetén a Hatóság honlapjáról letölthető alkalmazással kell rögzíteni az Utasítás 32. pontjában foglaltakat.

VI. AZ ADATKEZELÉSEK MEGKEZDÉSÉNEK, AZ ÉRINTETTI JOGOK ÉRVÉNYESÍTÉSÉNEK ELJÁRÁSRENDJE

96. Az adatkezelés jogalapjának meghatározása során az Utasítás 36. pontjában foglaltak figyelembe vételével kell eljárni.

97. Az adatkezelés jogalapjának meghatározása esetén, amennyiben kétség merül fel, a személyi állomány tagja az adatvédelmi tisztviselővel köteles egyeztetni.

98. Az érintetti kör tájékoztatás az Utasítás 40. pontja szerint történik. Az érintetti tájékoztató az intézet honlapján és a KIOSZK rendszerben érhető el.

a) fogvatartott befogadása során a zárkában található Házirend megfelelő mellékletével, vagy a befogadó beszélgetésen átadott tájékoztató útján valósul meg,
b) új felszerelő esetén a kinevezést követően írásban tájékoztatni szükséges.

99. Az Utasítás 37-40. pontban foglaltak végrehajtásáért a szakterületi vezetők a felelősek.

100. Az adatvédelmi tisztviselő köteles időszakosan az adatkezeléseket, továbbá a nem kötelező adatkezeléseket legfeljebb háromévente felülvizsgálni. A jogszabályban meghatározottak alapján kell eljárni a kötelező adatkezelések esetében.

VII. AZ ADATVÉDELMI INCIDENS KEZELÉSE

101. Az adatvédelmi incidens észlelése esetén a személyi állomány tag köteles haladéktalanul a szakterületi vezető felé jelentést tenni.

102. A szakterületi vezetők kötelesek az adatvédelmi incidensről való tudomásszerzést követően haladéktalanul az adatvédelmi tisztviselő felé jelzéssel élni az Utasítás 45. pontjában foglaltaknak megfelelő módon.

103. Az adatvédelmi tisztviselő az Utasítás 46. pontjában foglaltakat haladéktalanul végrehajtja.

104. Az adatvédelmi tisztviselő az Utasítás 47., illetve 48. pontjában foglaltakról szükség esetén haladéktalanul intézkedik.

VIII. ADATBIZTONSÁGI INTÉZKEDÉSEK

105. Munkaidőn kívül zárva kell tartani az asztal fiókjait és egyéb (nem lemezből készült) dokumentumokat tartalmazó szekrényeket is, adatot tartalmazó vagy arra utaló iratot, dokumentumot, egyéb információt elzáratlanul (pl.: asztalon, szekrényen stb.) nem lehet hagyni.

106. A kulcsdobozt csak a kulcsdobozon feltüntetett személyek vehetik fel, a rendkívüli esetben történő felnyitás tényét jegyzőkönyv formájában dokumentálni kell, illetve takarítás céljából munkaidőn túl csak a takarító személyzet rendelkezhet bejárással a takarítási feladatok elvégzéséig.

107. Az egyes helyiségek zárására, a kulcsok tartására és kezelésére vonatkozó helyi rendelkezéseket maradéktalanul be kell tartani.

108. Amennyiben az irodát az ott dolgozó munkatárs elhagyja, azt kulcsra zárva kell tartani, oda más nem léphet be a távollétében.

109. Más szakterületek dolgozói az irodákba történő belépése és ott tartózkodása, csak az oda beosztott dolgozó jelenlétében engedélyezett.

110. A számítógépes végponti eszközön gondoskodni kell a felhasználó hosszabb inaktivitása során a kikényszerített kijelentkezésről, vagy az eszköz használhatóságának a korlátozásáról (billentyűzetblokkolás, jelszavas képernyő védelem stb.) A szükséges beállításokat az Informatikai Osztály végzi, a felhasználó azokat nem módosíthatja.

111. Működő számítógépes végponti eszköz üzemképes állapotban, felügyelet nélkül nem maradhat. A felhasználó a helyiség elhagyásakor köteles a számítógépét zárolni, vagy kikapcsolni, illetve gondoskodni arról, hogy adathordozó ne maradjon felügyelet nélkül.

112. Telefonon személyi állományi taggal vagy fogvatartottal kapcsolatos konkrét információt kiadni, továbbá adatot közölni tilos.

113. A szakterületen található nyilvántartásokat, kimutatásokat az arra rendszeresített lemezszekrényekben kell elhelyezni, azokat kulccsal és szükség esetén pecsétlenyomattal ellátott falakattal is le kell zárni, a kulcsokat az iroda számozott kulcsdobozában kell tárolni.

114. Az informatikai rendszeren történő adatkezelés során maradéktalanul be kell tartani az informatikai biztonsági szabályok rendelkezéseit.

115. Az intézetben rendszeresített informatikai eszközöket csak felhasználói jogosultsággal rendelkező dolgozó használhat. A belépési jogosultsághoz tartozó felhasználói nevet és jelszót gondosan meg kell őrizni, azt tilos más személy tudomására hozni. A jogosultságokat a szakterületi vezetők kötelesek folyamatosan ellenőrizni, illetve naprakészen tartani.

116. A személyi és fogvatartotti állománnyal kapcsolatosan használt adatokat az adatkezelők csak a munkájukhoz szükséges mértékben használhatják, azt magáncélra felhasználni tilos.

117. A Robotzsaru rendszert, a Robotzsaru integrált ügyviteli, ügyfeldolgozó és elektronikus iratkezelő rendszer egységes és kötelező használatáról, jogosultsági rendjéről, a kapcsolódó adatvédelem előírásairól szóló 1-1/1/2013. (I.9.) OP intézkedésben, és a Váci Fegyház és Börtön iratkezelési rendszerének, valamint a Robotzsaru Neo és Nova programok használatának szabályozásáról szóló intézetparancsnoki intézkedésben foglaltak alapján kell kezelni. Az intézkedések átfogóan meghatározzák a Robotzsaru rendszerben alkalmazandó adatkezelési szabályokat és feladatokat.

118. A parancsnoki épület folyosóján elhelyezett központi nyomtató (VACI-PARA-EM01-PR20) használata során lehetővé kell tenni a dokumentumok személyes kóddal történő nyomtatását, az illetéktelen hozzáférés megelőzése végett.

119. „Az intézeti informatikai, számítástechnikai tevékenység szabályozása” tárgyú parancsnoki intézkedés és a BVOP Iratkezelési Szabályzata határozza meg az egyes elektronikus adatkezelő programrendszerek esetében az infrastruktúra és az alkalmazás rendszergazdai feladatköröket és felelősöket.

IX. A KÖZÉRDEKŰ ADATOK KÖZZÉTÉTELÉNEK ÉS A KÖZÉRDEKŰ ADATIGÉNYLÉSEK INTÉZÉSÉNEK ELJÁRÁSI SZABÁLYAI

120. Az Intézet köteles a honlapján közzétenni az Utasítás 5. melléklete szerinti adatokat az Info tv. 1. mellékletében meghatározott közlési és megőrzési időpontok szerint. A közzétételt a Személyügyi és Titkársági Osztály főelőadója végzi. A közzéteendő adatok rendelkezésre bocsátása a szakterületi vezetők feladata.

121. Közérdekű adat megismerésére irányuló kérelem beérkezése esetén a szakterületi vezető köteles azonnal tájékoztatni az adatvédelmi tisztviselőt.

122. Az adatvédelmi tisztviselő a közérdekű adatigénylést megvizsgálja, segítséget nyúlt a választervezet elkészítésében, a kijelölt ügyintéző gondoskodik a BVOP-ra felterjesztéséről jóváhagyást követően az adatigénylő részére a megküldésről az Utasításban meghatározott határidőn belül.

ELEKTRONIKUS MEGFIGYELÉSI RENDSZER

123. Az Intézet területén működő kamerarendszerek felvételei a bv. szerv külső és belső biztonsága, a bűnmegelőzés vagy bűnüldözés érdekében, valamint fegyelmi, etikai vétségek, a munkajogi és munkavédelmi kötelezettségek elmulasztásának megelőzése és feltárása

céljából – beleértve minden esetben az ellenőrzést és a felügyeletet is – továbbá az érintett vagy mások jogainak védelme érdekében használhatók.

124. Az Intézet által működtetett elektronikus megfigyelési eszközökre, továbbá a személyi állomány technikai ellenőrzésére külön szabályok az irányadóak. Jelen szabályzat kiadásakor e tárgyban a belügyminiszter irányítása alá tartozó rendvédelmi feladatokat ellátó szervek hivatásos állományú tagjai esetében a technikai ellenőrzés szabályairól szóló 23/2015. (VI. 15.) BM rendelet, a szolgálat alatt birtokban tartható tárgyak, eszközök körének korlátozásáról és a technikai ellenőrzés szabályairól 48/2020. (IX. 30.) BVOP utasítás előírásai alkalmazandóak.

125. A rendszerben tárolt adatok kiírását, felhasználását az intézetparancsnok engedélyezheti. A digitálisan rögzített adatok jelen intézkedésben meghatározott, szabályos feldolgozásáért (intézetparancsnoki felhatalmazás alapján) a biztonsági osztályvezető és az informatikai osztályvezető felelős. A rögzítésre kerülő kamerák, valamint a hozzáférésre jogosultak jegyzékét a biztonsági osztályvezető javaslata alapján az intézetparancsnok hagyja jóvá.

X. OKTATÁS

126. Az adatvédelmi tisztviselő az újonnan felvételre került személyek oktatását a személyügyi és titkársági osztályvezető tájékoztatása alapján oktatásban részesíti.

127. Az adatvédelmi tisztviselő az Intézet személyes adatok kezelését végző személyi állományának oktatását évente 2 alkalommal végzi, valamint az új belépők vonatkozásában soron kívül.

128. Az adatvédelmi tisztviselő az adatvédelmi tárgyú szabályokat és más kapcsolódó szabályokat a személyi állomány részére elektronikusan hozzáférhetővé teszi a belső informatikai rendszerben, valamint gondoskodik azok szükség szerinti aktualizálásáról.

XI. ZÁRÓ RENDELKEZÉSEK

129. Jelen intézkedés a kiadását követő napon lép hatályba. Ezzel egyidejűleg hatályát veszti az Adatvédelmi és Adatbiztonsági Szabályzatról szóló 55/2019. számú intézetparancsnoki intézkedés.

130. Jelen intézkedést a személyi állomány teljes terjedelemben köteles megismerni és alkalmazni.

Dr. Füzesi Viktor bv. ezredes, bv. tanácsos
intézetparancsnok

Készítette: Drobinoha Teréz c. bv. alezredes
Hozzáférhető a helyi számítógépes hálózat Belső Információs Rendszer Pk. intézkedések menüjében

ZÁRADÉK

A dokumentum elektronikus aláírással hitelesített

30532-3/9-1/2021.int.