III. AGGLOMERÁCIÓS KÖZPONT
SZEGEDI FEGYHÁZ ÉS BÖRTÖN

Száma: 30528-3/ /2024. int.

A SZEGEDI FEGYHÁZ ÉS BÖRTÖN PARANCSNOKÁNAK

30528-3/ /2024. int.

INTÉZKEDÉSE

A személyes adatokra vonatkozó adatvédelmi és adatbiztonsági feladatokról

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

intézkedést

adom ki.

I. Fejezet
Általános rendelkezések

1. Jelen intézkedés célja, hogy a Szegedi Fegyház és Börtön 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.) BVOP utasítással (a továbbiakban: Szabályzat), 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. törvény rendelkezései irányadók.

5. Az Intézet személyes adat kezelését (a továbbiakban: adatkezelést) az I., II., III. számú objektumaiban, továbbá az intézet objektumai mellett működő gazdasági társaságok fogvatartotti munkahelyei tekintetében végez.

6. Jelen intézkedés - a foglalkoztatási jogviszonyra vagy szerződéses jogviszonyra tekintet nélkül - azon munkatársakra (a továbbiakban: adatkezelést végző munkatárs) 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 (rendszergazda),
b) személyes adatokat tartalmazó papír alapú iratokat, vagy más adathordozót (a továbbiakban: okirat) kezelnek.

7. Az adatkezelést végző munkatársak 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.

8. Az adatkezelést végző munkatársak 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 adatokat nem kérhetik le,
b) az adatokról nem készíthetnek másolatot, kivéve az előírt biztonsági mentéseket,
c) az adatokat nem nyomtathatják ki, azok a nyomtatás után nem maradhatnak felügyelet nélkül,
d) az adatokat nem továbbíthatják, illetve azokat nem küldhetik el e-mailben,
e) az adatokhoz nem engedhetnek illetéktelen hozzáférést sem közvetlenül a számítógépnél, sem hálózaton vagy interneten keresztül, vagy okirat formájában,
f) az adathordozókat nem vihetik ki a bv. szerv területéről,
g) az adatokat nem hozhatják arra nem jogosult tudomására.

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

10. Az adatokat (pl. szövegszerkesztővel és táblázatkezelővel írt dokumentumok) az adatkezelést végző munkatársak az előírt helyre mentik, annak érdekében, hogy az adat a

biztonsági mentésbe bekerüljön; az ideiglenes munka állományok törlésére a végleges anyag elkészültekor intézkednek.

11. Ideiglenes adatmásolatokat, próbanyomtatásokat, elrontott nyomtatásokat a munka végeztével az adatkezelést végző munkatársak megsemmisítik, annak érdekében, hogy adat illetéktelenek számára ne legyen kinyerhető.

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

13. A hardver karbantartás alkalmával és eseti meghibásodások esetén a munkára kötött szerződés tartalmazza az esetenként és speciális célból az adatokhoz férők jogosultságait - pl. szoftverfejlesztő -, gondoskodva arról, hogy az adatok csak a szükséges mértékben és ideig legyenek ezen személyeknél, akik a munkájuk végeztével minden náluk lévő, a bv. szerv tulajdonát képező adatot kötelesek megsemmisíteni.

14. 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. Fejezet
Az adatvédelmi nyilvántartás, adatvédelmi hatásvizsgálat és előzetes konzultáció

15. A bv. szervek által kezelt, a Szabályzat 17. pontja szerinti adatvédelmi nyilvántartás vezetéséről az adatvédelmi tisztviselő gondoskodik, az adatkezelés tekintetében illetékes szakterület (szervezeti elem vagy külön meghatározott felelős személy) (a továbbiakban: illetékes szakterület) írásbeli tájékoztatása alapján.

16. A Szabályzat 18. pontja illetve 1. melléklete szerinti adatvédelmi adatlap elkészítése, illetve a Szabályzat 19. pontja szerinti felülvizsgálata, aktualizálása az illetékes szakterület feladata.

17. A Szabályzat 26-35. pontja szerinti adatvédelmi hatásvizsgálat (előzetes kockázatbecslés) és előzetes konzultáció érdekében az adatvédelmi tisztviselőt az új, vagy a korábbiaktól eltérő adatkezelést előíró vagy eredményező jogszabály vagy belső szabályozó eszköz, eljárásrend, eszköz vagy technológia bevezetéséről vagy változásáról az illetékes szakterület a Szabályzat 28. pontja [hatásvizsgálat alóli mentesség esetei] figyelembevételével tájékoztatja. Az adatvédelmi hatásvizsgálat elrendeléséről, illetve az előzetes konzultáció kezdeményezéséről a parancsnok az adatvédelmi tisztviselő javaslatára dönt.

III. Fejezet
Az adatokba betekintés és az adat továbbításának, valamint a másolatkészítés iránti kérelmek, megkeresések ügyintézésének rendje

18. Az érintett (így személyi állomány tagja, fogvatartott vagy más személy, akinek a bv. szerv az adatait jogalap alapján kezeli) saját adatait - a törvényben foglalt kivételekkel - megismerheti, illetve részére az ilyen adatokat tartalmazó iratokról másolat adható ki.

19. Az adatkezelést végző munkatárs az adattovábbítás ügyintézése során az arra vonatkozó jogalapot (felhatalmazást) érdemben vizsgálja az Adatvédelmi Rendelet, illetve jogszabály konkrét rendelkezésére (jogszabály címe és száma, § sorszám és bekezdés, pont) vonatkozóan, illetve az adattovábbítást az adattovábbítási nyilvántartásban rögzíti. Hozzájáruláson alapuló adatkezelés - így különösen, az érintett adatainak továbbítása - esetén az adatkezelő hozzájáruló nyilatkozat eredeti példányát az ügy iratai között helyezi el. Az adatszolgáltatásra irányuló megkeresés, kérelem tisztázatlansága, vagy a meghatározottaktól eltérő hiányossága esetén az adatkezelő az adatkérő felé hiánypótlási felhívás elkészítéséről és megküldéséről gondoskodik, melyben az érintettre vonatkozó személyes adat nem továbbítható.

20. Az érintett az adatairól történő másolat kiadása során - amennyiben jogszabály alapján a költségek viselésére kötelezett - nyilatkozik a költségek vállalásáról. A kérelem intézése során az ügyintézésre kijelölt szervezeti elem (illetékes szakterület) ügyintézője meghatározza a másolat tárolásához szükséges adathordozó jellegét és mennyiségét, majd a gazdasági osztály az önköltségi szabályzat alapján nyilatkozik a térítési díjról. Amennyiben az érintett fogvatartott, a konkrét összeg levonását a letéti pénzéből kéri.

21. Az érintett által nem megismerhető adatokat, amennyiben azok az elektronikus adatok esetén összességben egységet képeznek (pl. a számítógépben rögzített szakterületi vélemény) az irat nyomtatásakor az adatkezelő kiszerkeszti vagy másoláskor kitakarása felismerhetetlenné teszi. Az adatok felismerhetetlenné tételéről a kérelem elintézésére kijelölt szervezeti elem ügyintézője gondoskodik.

22. A megismerés, másolat kiadása és adattovábbítás esetén az adatot kezelő, feladattal érintett szervezeti egység gondoskodik a szükséges ügymenetről.

23. Személyes adatokról telefonon vagy egyéb, nem ellenőrizhető és dokumentálható módon felvilágosítás nem adható, e-mailben érkező megkeresés és adattovábbítás esetén erről az érintett figyelmét az adatkezelő kifejezetten felhívja, melyben adatainak e módon történő továbbításához az érintettnek kifejezetten hozzá kell járulnia.

IV. Fejezet
Az érintettek jogainak érvényesülése és az ahhoz kapcsolódó nyilvántartások

24. Az érintettek személyes adataira vonatkozó, külső szervek vagy személyek felé történő adattovábbításokról, vagy annak megtagadásáról, továbbá az érintettek általi, saját adataikra vonatkozó betekintésekről vagy megtagadásról az érintett személy szerint illetékes szervezeti elem a „Betekintési nyilvántartás”, illetve „Adattovábbítási nyilvántartás” megnevezésű nyomtatványt vezet. *(Szabályzat 20, 21. pont, Szabályzat 2.- 3. sz. melléklet).*

V. Fejezet
A fogvatartottak adatainak kezelésével kapcsolatos egyes külön rendelkezések

25. Amennyiben az érintett fogvatartott, úgy adatainak megismeréséről, illetve a fogvatartási jogviszonyt érintő irat másolat kiadásának megtagadásáról az ügyintézésre kijelölt szervezeti elem vezetője, feladatkörében határozatot hoz. E rendelkezés a fogvatartási jogviszony

megszűnését követően előterjesztett kérelmekre - így a volt fogvatartott, vagy az elhunyt fogvatartott személy hátramaradt hozzátartozója által előterjesztett kérelmekre - is vonatkozik.

26. A fogvatartott a büntetés-végrehajtás által kezelt saját adatainak megismerésére - az adatkezelés jogalapjától függően - jogszabály, különösen a Bv. tv. 26. §, valamint a Bvsz. tv. 30. § rendelkezése szerint jogosult; a fogvatartási jogviszonyt érintő másolat kiadási kérelmeket a feladatkörrel rendelkező szervezeti elem (illetékes szakterület) a Bv. tv. szerint intézi; az egészségügyi adatok megismerésének és továbbításának feltételeiről külön egészségügyi tárgyú jogszabályok rendelkeznek.

27. A fogvatartott adatainak a Bvsz. tv. 29. § (1) bekezdés szerinti, a miniszter, a bíróság, az ügyészség, a rendőrség és az egyéb nyomozó hatóságok, és az előkészítő eljárást folytató szervek, a nemzetbiztonsági szolgálatok, valamint a Nemzeti Adatvédelmi és Információszabadság Hatóság részére történő mérlegelés nélküli továbbítás előkészítéséről - az adatkezelés törvényi feltételeinek fennállása esetén - a feladatkörrel rendelkező szervezeti elem gondoskodik, az intézet által kezelhető adatainak teljes körére vonatkozóan, a megkeresés szerinti terjedelemben.

28. A 27. pont körén kívül más szervek vagy személyek a feladataik ellátásához, illetve a jogaik érvényesítéséhez szükséges fogvatartotti adatokat ismerhetik meg, hivatalból vagy kérelemre. Az adatszolgáltatásra irányuló kérelem esetén az adatkérő az adatkérés indokát, jogszabályi alapját, illetve az adatszolgáltatáshoz fűződő érdek igazolását megjelölni, ennek hiánya esetén a feladatkörrel rendelkező szervezeti elem (illetékes szakterület) a hiánypótlásra felhívásra intézkedik. Az adatszolgáltatásra irányuló kérelem tisztázatlansága, vagy a meghatározottaktól eltérő hiányossága esetén az adatkezelő az adatkérő felé hiánypótlási felhívás elkészítéséről és megküldéséről gondoskodik, melyben az érintettre vonatkozó személyes adat nem továbbítható.

29. A személyi állomány a fogvatartottak adatait tartalmazó papír alapú nyilvántartásokat, személyes adatokat tartalmazó iratokat kizárólag a legszükségesebb, jogszabály vagy közjogi szervezetszabályozó eszköz által meghatározott esetben kezelheti. A fogvatartottakkal közvetlenül foglalkozó személyi állományi tagokra és az olyan szolgálatteljesítési helyekre vonatkozóan, ahol fogvatartottak ideiglenes jelleggel megfordulhatnak, papír alapú iratok külön meghatározás szerint, valamint akkor kezelhetőek, ha elektronikus úton annak kezelése nem valósulhat meg.

30. Amennyiben a kizárólag elektronikus úton megvalósuló hiteles nyilvántartás és adatmegismerés feltételei fennállnak, úgy – eltérő rendelkezés hiányában - papír alapú nyilvántartás nem alkalmazható, azt kinyomtatni nem lehet.

31. A jogosulatlan hozzáférések megelőzése, az adatvédelmi incidens bekövetkezési kockázatának kizárása érdekében a szolgálati helyiségeket zárva kell tartani. Azon szolgálati helyek esetében, melyek nem zárhatók, ott a szolgálati okmányok, adatvédelmi szempontból aggályos dokumentumok, fegyverzeti-, valamint egyenruházati anyagok, felszerelések, lezáratlan informatikai eszközök őrizetlenül nem hagyhatók.

VI. Fejezet
Egyes sajátos helyzetben lévő személyek adatainak kezelésével kapcsolatos egyes külön rendelkezések

1. Cím
A panaszos és a közérdekű bejelentő adatainak védelme

32. A panaszokról és a közérdekű bejelentésekről szóló törvény szerinti panasz vagy közérdekű bejelentés esetén, ha a panaszos vagy a közérdekű bejelentő személye azonosítható és a körülményekből adódóan a személyes adatai nyilvánosságra hozatalának indokoltsága merül fel, ezt megelőzően a panaszban, közérdekű bejelentésben feladatkörrel rendelkező szakterület az érintettet nyilatkoztatja, hogy az érintett hozzájárul-e személyes adatainak nyilvánosságra hozatalához. A nyilatkozatot a panasz, közérdekű bejelentés iratai között kell elhelyezni.

2. Cím
A fogvatartottra vonatkozó bejelentést tett személy adatainak védelme

33. A fogvatartottra vonatkozó, az intézet rendje és biztonsága szempontjából jelentős tényre vagy körülményre utaló adatot tartalmazó bejelentést a bejelentő (a továbbiakban: bejelentő) megjelölésével a számítógépes fogvatartotti rendszer vélemények-feljegyzések menüpontja alatt kell rögzíteni. Amennyiben a 34. pont szerinti zárt adatkezelést kért a bejelentő, csak a zárt adatkezelés ténye, valamint a bejelentő adatait tartalmazó eredeti irat iktatási száma rögzíthető a nyilvántartásban.

34. Ha a bejelentő személye azonosítható, a bejelentés szerint feladattal rendelkező munkatárs nyilatkoztatja, hogy kéri-e személyes adatainak zártan kezelését. Ha a bejelentő a személyes adatainak zártan kezelését kéri, biztosítania kell, hogy a személyes adatai ne jussanak az elítélt vagy az egyéb jogcímen fogvatartott tudomására. Az adatok zártan kezelése esetén a bejelentő azonosítására alkalmas adatait zárt borítékban kell a fogvatartotti anyaggyűjtőben elhelyezni. A borítékon jól látható módon kell megjelölni, hogy zártan kezelt adatokat tartalmaz. Amennyiben a fogvatartott a saját adatait meg kívánja ismerni, a bejelentő adatait védő, zárt boríték biztonságos megőrzéséről kell gondoskodni.

35. Ha a bejelentő személye nem azonosítható vagy a fogvatartottra vonatkozó, az intézet rendje és biztonsága szempontjából jelentős tényre vagy körülményre utaló adatot tartalmazó bejelentés ellenőrzése más ok miatt nem lehetséges, a bejelentést a fogvatartotti nyilvántartásban annak nem ellenőrzött jellegére való utalással kell rögzíteni.

3. Cím
A sértett adatainak védelme

36. A fogvatartott intézetelhagyására vonatkozó, a Bv. tv. 13. § szerinti sértetti tájékoztatási kérelmet a nyilvántartási osztály munkatársa a fogvatartott számítógépes nyilvántartásában rögzíti. A kérelmet, a sértett nevét és lakcímét zártan kell kezelni; az iratokat a fogvatartott nyilvántartási anyaggyűjtőjében, zárt borítékban kell elhelyezni. A borítékon jól látható módon kell megjelölni, hogy zártan kezelt adatokat tartalmaz. A zártan kezelendő sértetti kérelemre tekintettel, a kérelem tényére való feljegyzés a papír alakú fogvatartotti nyilvántartási anyagban nem tehető. Amennyiben a fogvatartott adatait saját maga, vagy más meg kívánja ismerni, a zárt adatok, és a zárt boríték biztonságos megőrzéséről kell gondoskodni.

VIII. Fejezet
Az adatvédelmi incidenssel kapcsolatos rendelkezések

37. A Szabályzat 43. pontja szerinti adatvédelmi incidens vagy annak gyanúja esetében az érintett személy(ek) adatkezelése tekintetében feladat és hatáskörrel rendelkező szakterület vezetője (felelőse) haladéktalanul jelentést tesz a bv. szerv vezetője számára, a Szabályzat 44-48. pontja szerintiek érvényesülése érdekében.

IX. Fejezet
A veszélyhelyzethez kapcsolódó védelmi intézkedések

38. A bv. szervek feladatainak ellátásához szükséges és elégséges adatkezelést és a személyes adatok védelmét rendkívüli esemény alkalmával, veszélyhelyzetben, illetve katasztrófahelyzetben (a továbbiakban: veszélyhelyzet) is biztosítani kell. A háttérrendszert úgy kell kialakítani, hogy maximális adatbiztonságot garantáljon, egy katasztrófahelyzet esetében adatvesztés ne következzen be, illetve ha ez mégis megtörténik, ennek mértéke minimális legyen.

39. Az informatikai szaktevékenységet ellátó munkatárs gondoskodik a megelőző adatbiztonsági intézkedésekként a napi biztonsági mentésekről. Az adatállományokról készített biztonsági mentések esetében elvárás, hogy az érzékeny személyes adatokat, például a személyi nyilvántartás, vagy a fogvatartotti jogviszonyra vonatkozó adatokat titkosított formában lehessen menteni, illetve a veszélyhelyzet utáni helyreállítási folyamat során ez a titkosítási algoritmus rendelkezésre álljon.

40. A veszélyhelyzetet követően rendelkezésre kell állnia az utolsó biztonsági mentéseket tartalmazó adathordozóknak, és az adatokat vissza kell tölteni a rendszerbe. Alapvetően minden rendszer esetében szükséges az adatokról mentés készítése, de a rendszerek kritikusságához kapcsolódóan kell elvégezni a mentések tárolását.

41. Annak érdekében, hogy a biztonsági mentéssel vissza nem állítható adatok mennyisége minimálisra csökkenjen, az adatok ne vesszenek el véglegesen, az adatkezelők által kritikusnak nyilvánított adatok esetében - szükség esetén, különösen veszélyhelyzetben vagy annak lehetősége esetén - intézkedni kell az adatkezelés alatti folyamatos mentésre az adatkezelők által meghatározott időközönként az adatbevitel és feldolgozás közben. Az így elvégzett mentések esetén arányosan csökkenthető, minimalizálható az elveszett adatok köre. Az adatkezelőknek intézkedni kell a legutolsó mentés óta elveszett adatok újra bevitelére és feldolgozására.

42. Az ügyviteli-informatikai rendszerek helyreállíthatóságának biztosítására az adatok mentésén túl a teljes rendszerkörnyezet mentéséről is gondoskodni kell. A mentési rend szabályozza részletesen az adatok és a rendszerek mentésével kapcsolatos teendőket. A minősített időszaki feladatokat a szervezeti egységek felkészülési tervei tartalmazzák.

43. Az adatok biztonságával kapcsolatos részletes szabályokat az informatikai biztonsági szabályzatról szóló OP utasítás tartalmazza.

44. Egy katasztrófa utáni helyreállítási folyamat esetében az informatikai és nem informatikai helyreállítási tevékenységeket az Intézet esetén az informatikai szakfeladatokat ellátó

munkatárs, a titkársági osztályvezető koordinálja.

X. Fejezet
Vegyes rendelkezések

45. A büntetőeljárás esetén az iratismertetéseket a fogvatartottak és mások pl. sértettek adatainak védelmével kell tartani, különösen ügyelve arra, hogy az iratok őrizetlenül, illetve illetéktelenek számára ne válhassanak hozzáférhetővé.

46. Az intézetben tevékenységet végző és a fogvatartottak személyes adatainak birtokába kerülő külsős személyeket (pl. együttműködő szervezetek tagjai, kutatók, hallgatók) a be és kilépés, valamint az intézetben tartózkodás szabályairól történt tájékoztatással egy időben figyelmeztetni kell arra, hogy tevékenységüket a személyes adatok védelmével kapcsolatos jogszabályok betartásával végezhetik. A figyelmeztetés dokumentálásáról az adott tevékenység szerint feladatkörrel rendelkező szervezeti elem vezetője, vagy vezetői közvetlen munkatárs gondoskodik, illetve az erre vonatkozó figyelmeztetést a megkötendő együttműködési megállapodásokban, intézetlátogatási engedélyekben is szerepeltetni kell.

47. A jogszabály alapján alkalmazott elektronikus megfigyelési eszköz alkalmazásának szabályait külön intézkedés tartalmazza.

48. A személyi állománynak körültekintéssel, az adott szakterületre vonatkozó általános és speciális jogszabályi rendelkezésekbe foglaltak szerint, mérlegelve kell eljárnia intézkedése, megnyilvánulása során, a fogvatartottak részéről elektronikai eszközzel esetlegesen tervezett-, a személyi állomány tagjának személye ellen irányuló, provokatív, zsaroló, megfélemlítő cselekmény megelőzése érdekében.

49. A közérdekű és közérdekből nyilvános adatokra vonatkozó igények intézésének rendjét külön meghatározás tartalmazza.

XI. Fejezet
Záró rendelkezések

50. Jelen intézkedés a kiadás napját követő harmadik napon lép hatályba, mellyel együtt a személyes adatokra vonatkozó adatvédelmi és adatbiztonsági feladatokról szóló 30528/59/2019. int. intézkedéshatályát veszti.

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

Kopcsik Károly bv. dandártábornok
büntetés-végrehajtási főtanácsos
parancsnok

ZÁRADÉK

A dokumentum elektronikus aláírással hitelesített

30528-3/28/2024.int.