V. AGGLOMERÁCIÓS KÖZPONT
CSENGERI ORSZÁGOS BÜNTETÉS-VÉGREHAJTÁSI INTÉZET TELEPHELYE
JÁSZ-NAGYKUN-SZOLNOK VÁRMEGYEI BÜNTETÉS-VÉGREHAJTÁSI INTÉZET

A JÁSZ-NAGYKUN-SZOLNOK VÁRMEGYEI BÜNTETÉS-VÉGREHAJTÁSI INTÉZET PARANCSNOKÁNAK

3/2026.

I N T É Z K E D É S E

Az adatvédelmi és adatbiztonsági szabályzatról

A büntetés-végrehajtási szervezet belső szabályozási tevékenységéről szóló 2/2013. (IX. 13.) BVOP utasítás 3. pontja alapján – figyelemmel az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény, az Európai Parlament és a Tanács (EU) 2016/679 rendelete, valamint a büntetés-végrehajtási szervek Adatvédelmi és Adatbiztonsági Szabályzatáról szóló 25/2025 (XI. 20.) BVOP utasítás rendelkezéseire – az alábbi

i n t é z k e d é s

kerül kiadásra:

I. ÁLTALÁNOS RENDELKEZÉSEK

1. Az adatvédelmi tisztviselő feladatait az Info.tv.25/L, 25/M, 25/N §-ok alapján látja el. Az adatvédelmi tisztviselő feladata továbbá, az adatkezelési szabályzat szükséges módosításának, aktualizálásának előkészítése.

2. 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.

II. RÉSZLETES RENDELKEZÉSEK

1. Az adatkezeléssel kapcsolatos nyilvántartások

3 Az intézet adatvédelmi tisztviselője, az intézet által kezelt személyes adatokról a RobotZsaru integrált ügyviteli, ügyfeldolgozó és elektronikus iratkezelő rendszerben e célból létrehozott iktatókönyvben adatvédelmi nyilvántartást vezet.

4 A személyes adatokat tartalmazó adatkezelések adatvédelmi nyilvántartásba történő rögzítését az érintett szakterület adatkezelője jelen intézkedés 1. melléklet szerinti adatlapján kezdeményezi az adatvédelmi tisztviselőnél.

5 A szakterületek adatkezelői kötelesek gondoskodni, az általuk kezelt személyes adatok vonatkozásában az adatvédelmi adatlap folyamatos felülvizsgálatáról. Az adatlapokban észlelt esetleges eltérések esetén az adatfeldolgozó az aktualizált adatlapot haladéktalanul továbbítja az adatvédelmi tisztviselő részére.

6. A szakterületek által kezelt személyes adatokba történő betekintésekről, illetve az adatokra és azok kezelésére vonatkozó információk érintett részére való rendelkezésre bocsátásáról a szakterület a 2. melléklet szerinti betekintési nyilvántartást vezet.

7. A betekintési nyilvántartásnak tartalmaznia kell:
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.

8. Az intézet szakterületein 3. melléklet szerinti adattovábbítási nyilvántartást kell vezetni, amelyhez csak az adott szakterület adatkezelésre jogosult személyei és az intézet adatvédelmi tisztviselő férhet hozzá. Az intézeti adatvédelmi tisztviselő az intézeti szinten összesített adattovábbítási nyilvántartáshoz is hozzáfér. Az adattovábbítási nyilvántartás fenti módon való kialakításáért az informatikai csoportvezető (GEI) a felelős.

9. Az intézet szakterületein, 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.

10. Az adattovábbítási nyilvántartásnak tartalmaznia kell:
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).

11. Az Intézet a szakterületek általuk kezelt adatokkal összefüggésben felmerült adatvédelmi incidensekről a 4. melléklet szerinti jegyzőkönyvekből álló nyilvántartást vezet, a nyilvántartás vezetése az adatvédelmi tisztviselő feladata.

12. Az adatvédelmi incidensek rögzítésére szolgáló jegyzőkönyvnek tartalmaznia kell:
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.).

13. A bv. szervek az elutasított közérdekű adatigénylésekről, valamint azok indokairól nyilvántartást vezetnek

14. 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.

2. Adatvédelmi tisztviselő hatásköre és feladatai

15. Az adatvédelmi tisztviselő eljár a részére munkaköri leírásában átruházott feladatkörökben. Az átruházott feladatkörök tekintetében, amennyiben jogszabálytól történő eltérést észlel, adatkezelés jogszerűsége érdekében szükséges intézkedések megtételére az Intézet parancsnoka a felelős.

16. Az adatvédelmi tisztviselő akadályoztatása esetén az Intézet parancsnoka helyettest jelöl ki, akinek adatvédelemmel összefüggő feladatkörei megegyeznek az adatvédelmi tisztviselő feladatköreivel.

17. Adatvédelmi tisztviselő feladatai:

a) tájékoztatást nyújt és szakmai tanácsot ad a vonatkozó Európai Uniós és hazai jogszabályokban foglalt adatvédelmi rendelkezések szerinti kötelezettségekről;

b) figyelemmel kíséri az adatvédelemmel és információszabadsággal összefüggő jogszabályváltozásokat, ellenőrzi a személyes és közérdekű adatok kezelésére vonatkozó jogszabályok és belső szabályozó eszközök érvényesülését;

c) közreműködik, illetve segítséget nyújt az adatkezeléssel összefüggő döntések meghozatalában, valamint az érintettek jogainak biztosításában;

d) közreműködik az adatvédelmi hatásvizsgálat lefolytatásában;

e) elkészíti az adatkezelő szerv adatvédelmet érintő belső szabályozó eszközeinek tervezetét;

f) vezeti az adatkezelő szerv adatvédelmi nyilvántartását, valamint az adatvédelmi incidensek nyilvántartását;

g) kivizsgálja a bv. szerv adatkezelésével összefüggésben érkező panaszokat, kifogásokat;

h) az adatkezelő szerv vezetőjének megbízásából ellenőrzi az adatkezelő szervnél az adatvédelmi követelmények megtartását, adatvédelmi incidens bekövetkezése esetén haladéktalanul intézkedik annak kezelésére, valamint szükség esetén ellátja a Hatóság részére való bejelentéssel, illetve az érintett tájékoztatásával kapcsolatos feladatokat; indokolt esetben az adatkezelő szerv vezetőjénél kezdeményezi a felelősség megállapításához szükséges eljárás lefolytatását;

i) a bejelentés-köteles incidensekről a jegyzőkönyv felterjesztésével jelentést tesz, továbbá a honlapon közzététellel megvalósuló érintetti tájékoztatás esetén annak tervezetét jóváhagyás céljából azonnal felterjeszti a BVOP adatvédelmi tisztviselőjének;

j) tájékoztatja a Hatóságot az adatvédelmi tisztviselő adatairól (név, postai és elektronikus levélcím) és azok változásáról, továbbá gondoskodik ezen adatok nyilvánosságra hozataláról;

k) gondoskodik a bv. szerv személyi állományának oktatásáról;

l) felügyeli az adatkezelő szerv adattovábbítási tevékenységét, különös tekintettel a nemzetközi együttműködés keretében továbbítandó személyes adatokra, felkérésre adatvédelmi szempontból állást foglal az adatok továbbításának jogszerűségével kapcsolatban;

m) közreműködik a kérelem tárgyában érintett szakterülettel az érintett hozzáférési joga gyakorlására vonatkozó kérelmére, illetve a közérdekű adat megismerésére irányuló kérelmekre adandó válasziratok elkészítésében;

n) a beérkezett közérdekű adatigénylést haladéktalanul, az elkészített választervezetet az adatigénylés beérkezését követő 8 napon belül felterjeszti a BVOP adatvédelmi tisztviselője részére;

o) az elutasított közérdekű adatigénylések számáról és az elutasítások indokairól nyilvántartást vezet, melynek éves összesítését a tárgyévet követő év január 10-ig felterjeszti a BVOP adatvédelmi tisztviselője részére;

p) ellenőrzési tervet készít, amely alapján, továbbá szükség esetén azon felül is ellenőrzi a személyes és közérdekű adatok kezelésére vonatkozó jogszabályok és belső szabályozó eszközök érvényesülését;

18. Az adatvédelmi tisztviselő, adatvédelemmel kapcsolatos feladatköreinek ellátása során folyamatosan együttműködik, az adatkezeléssel érintett szakterületekkel, Informatikai csoportvezetővel (GEI).

19. Amennyiben az adatvédelmi tisztviselő az adott feladat ellátása kapcsán összeférhetetlennek minősül, arról haladéktalanul jelentést tesz a főigazgató részére, ez esetben az ügyben a helyettes jár el. A helyettes összeférhetetlensége vagy akadályoztatása esetén a főigazgató jelöli ki az ügyben a feltételeknek megfelelő eseti helyettest.

3. Adatvédelmi hatásvizsgálat és előzetes konzultáció

20. Az Intézet tekintetében újnak, vagy a korábbitól eltérőnek minősülő adatkezelést meghatározó, vagy eredményező jogszabály, belső szabályzó, eljárás rend, eszköz illetve technológia bevezetését, illetve változtatását megelőzően az adatvédelmi tisztviselő kockázatbecslést végez.

21. A kockázatbecslés végrehajtása során az adatvédelmi tisztviselő megvizsgálja, az általános adatvédelmi rendelet, infótörvény, illetve a hatósági iránymutatás alapján, az adatkezeléssel járó kockázat mértékét, az érintettek alapvető jogainak érvényesülése vonatkozásában. A kockázatbecslés végrehajtása során, amennyiben szükséges az adatvédelmi tisztviselő véleményezést kér az adatkezelésben érintett szakterületektől, az adatkezeléssel járok kockázatok azonosítása érdekében. Az adatvédelmi tisztviselő a kockázatbecslésről jelentést készít, amelyet jóváhagyás céljából az Intézet parancsnoka elé terjeszt.

22. Az adatvédelmi hatásvizsgálat lefolytatásától el lehet tekinteni, amennyiben az adatvédelmi tisztviselő az alábbiakat állapítja meg:

a) A tervezett adatkezelés valószínűsíthetően nem jár magas kockázattal.

b) A tervezett adatkezelés a Hatóság által meghatározott kivételi körbe tartozik.

c) A tervezett adatkezeléssel megegyező adatkezelés tekintetében elvégzett hatásvizsgálat rendelkezésre áll.

d) A jogszabályban előírt adatkezelés tekintetében, a jogalkotó már a hatásvizsgálatot már lefolytatta.

23. A hatásvizsgálat lefolytatása, illetve mellőzése a parancsnok hatáskörébe tartozik, amelyről az adatvédelmi tisztviselő által megállapítottak figyelembevételével dönt. Az adatvédelmi hatásvizsgálat elrendelése esetében, figyelembe véve annak tárgyát, illetve formáját, a hatásvizsgálatban résztvevő személyek, valamint szakterületek körét a parancsnok határozza meg.

24. Amennyiben indokolt a hatásvizsgálat lefolytatásának mellőzése, annak indokait az adatvédelmi tisztviselő jelentés formájában írásban rögzíti, valamint csatolja a kockázatbecslés iratanyagához.

25. Az adatvédelmi hatásvizsgálat elrendelése esetén az azt végrehajtó csoport, tekintettel az általános adatvédelmi rendeletre, info. tv.-re, illetve a hatósági iránymutatásra, a hatóság honlapjáról letölthető hatásvizsgálati szoftver („PIA software") alkalmazásával végrehajtja a hatásvizsgálatot. A hatásvizsgálat során a csoport rögzíti a szoftver alkalmazásával, az adatkezelési művelet leírását, az adatkezelés célját, az adatkezelés céljára figyelemmel elvégzett adatkezelési műveletekre vonatkozó szükségességi és arányossági vizsgálat eredményét, az érintet alapvető jogainak érvényesülését fenyegető kockázatot, valamint a kockázatkezelést célzó adatbiztonsági intézkedések részletes leírását és értékelést.

26. Az az adatvédelmi hatásvizsgálat lefolytatását követően a hatásvizsgálat eredményéről a csoport jelentést készít, amely tartalmazza:

1.amely tartalmazza a hatásvizsgálat lefolytatásának okait,
2.hatásvizsgálatban résztvevők nevét, szerepét és felelősségi körét,
3.a „PIA software"-ben rögzített adatokat,
4.a megállapított kockázati szintet.

27. Amennyiben a hatásvizsgálat során megállapításra kerül, hogy a tervezett adatkezelés az érintettek alapvető jogainak érvénysülése tekintetében magas kockázatot jelent, vagy a hatóság honlapján közzétett hatásvizsgálati listán magas kockázatú minősítést kapott, a parancsnok konzultációt kezdeményez a Hatósággal.

28. Az összefoglaló jelentés tartalma alapján a parancsnok meghatározza az adatkezelés megvalósulásának nyomon követésében resztvevők körét, a résztvevő szakterületek, valamint az adatkezelés felülvizsgálatának gyakoriságát és módszerét.

29. Adatkezelés megkezdésének, illetve az érintetti jogok érvényesítésének eljárásrendje.

30. Az érintett személyes adatainak kezeléséhez történő hozzájárulását a későbbi igazolhatóság érdekében írásban kell rögzíteni.

31. Az adatkezelés megkezdése előtt, vagy az első adatkezelési művelet megkezdését követően az Intézet haladéktalanul az érintett rendelkezésére bocsájtja, az adatkezelő megnevezését és elérhetőségét, az adatvédelmi tisztviselő adatait, az adatkezelés célját, valamint az érintettet adatkezeléssel kapcsolatosan megillető jogokra, illetve azok érvényesítésére vonatkozó ismertetőt. Az adatkezelő továbbá írásban tájékoztatást nyújt az érintett részére, az adatkezelés jogalapjáról, a kezelt személyes adatok megőrzésének időtartalmáról, a kezelt személyes adatok továbbítása vagy tervezett továbbítás esetén az adattovábbítás címzettjeinek köréről, a kezelt személyes adatok gyűjtésének forrásáról és az adatkezeléssel összefüggő minden érdemi tényről.

32. Az érintetek 31. pontban foglaltakra vonatkozó tájékoztatása az adatkezelést végző szakterület feladata, amelynek megtörténtét írásban rögzít az érintett szakterület.

33. Az adatkezelésben érintett által előterjesztett, hozzáféréshez, helyesbítéshez, adatkezelés korlátozásához, vagy törléshez való joga érvényesítésre vonatkozó kérelem elbírálása, illetve megválaszolása az adatkezelést végrehajtó szakterület feladata.

34 Az Intézet által végrehajtott adatkezeléseket időszakosan felül kell vizsgálni, a felülvizsgálatnak ki kell terjednie, hogy az adatkezelés céljának megvalósulásához szükséges-e a személyes adatok kezelése, illetve megfelel-e az általános adatvédelmi rendelt és az info.tv. rendelkezéseinek. A jogszabályban meghatározott kötelező adatkezelés esetében a jogszabályban meghatározott gyakoriságban kell végrehajtani. Azon adatkezelés tekintetében, amelyek esetében a jogszabály felülvizsgálatot nem határoz meg, valamint a nem kötelező adatkezelések esetében legfeljebb háromévente felülvizsgálatot kell végrehajtani. A felülvizsgálat körülményeit, illetve eredményét írásban kell rögzíteni, amely iratot az adatvédelmi tisztviselő tíz évig megőriz.

4. Adatvédelmi incidensek bekövetkezése során alkalmazandó eljárásrend

35. Adatvédelmi incidens bekövetkezésének észlelése esetén az adatvédelmi incidensről az észlelő köteles haladéktalanul jelentést tenni a szakterületi vezető részére.

36. Az adatvédelmi incidens részére történő jelentését követően haladéktalanul tájékozódik az incidens körülményeiről, az adatvédelmi tisztviselő bevonásával felméri, hogy a bekövetkezett adatvédelmi incidens valószínűsíthetően kockázatot jelent-e az érintettek jogainak érvényesülése tekintetében, valamint haladéktalanul intézkedik a kárelhárítás, kárenyhítés érdekében.

37. Az adatvédelmi incidens bekövetkezéséről a szakterületi vezető haladéktalanul értesíti az adatvédelmi tisztviselőt, valamint a rendelkezésére bocsájtja az incidenssel kapcsolatos iratokat, illetve információkat, amennyiben az előzetes felmérés alapján valószínűsíthető kockázattal jár az adatvédelmi incidens.

38. Az adatvédelmi incidens bekövetkezéséről a szakterületi vezető írásban tájékoztatja az adatvédelmi tisztviselőt, amennyiben a felmérés során megállapításra került, hogy az incidens nem jár kockázattal.

39. Az 52. pontban meghatározott esetben az adatvédelmi tisztviselő a rendelkezésére álló iratok, illetve információk alapján, amennyiben szükséges az érintett szakterület bevonásával kockázatbecslést végez a bekövetkezett incidenssel kapcsolatban. Amennyiben a kockázatbecslés alapján az incidens kockázattal jár, az adatvédelmi tisztviselő 72 órán belül a hatóság honlapján, az incidens bejelentő rendszeren keresztül bejelentést tesz. Az incidens bejelentésével egy időben az adatvédelmi tisztviselő jelentést tesz az Intézet parancsnok részére a bekövetkezett adatvédelmi incidensről, valamint annak körülményeiről. Amennyiben az adatvédelmi incidens bejelentése határidőben nem teljesíthető, a bejelentésben fel kell tüntetni a késedelem okait.

40. Amennyiben a kockázatbecslés alapján az incidens magas kockázattal jár, és nem áll fent az általános adatvédelmi rendelet, illetve az info. tv.-ben meghatározott mentesülési okok egyike, az adatvédelmi tisztviselő haladéktalanul jelentést tesz az Intézet parancsnok részére illetve dokumentált módon tájékoztatja az érintetteket. Amennyiben az érintettek tájékoztatása aránytalan erőfeszítéssel járna, az adatvédelmi tisztviselő intézkedik a tájékoztatás közzétételéről az Intézet honlapján.

5. Hatósági ellenőrzés esetén alkalmazandó eljárásrend

41. Amennyiben az Intézet tekintetében a hatóság vizsgálatot, adatvédelmi hatósági eljárást, illetve titokfelügyeleti hatósági eljárást indít, az adatvédelmi tisztviselő köteles haladéktalanul jelentést tenni a BVOP adatvédelmi tisztviselője részére.

42. A hatósági vizsgálatban, illetve a titokfelügyeleti hatósági eljárásban érintett szakterület vezetője köteles a minősített adatok megismerését elősegíteni, illetve köteles a hatóság részére biztosítani:

a) a szükséges tájékoztatást szóban és írásban,

b) a személye adatokkal, közérdekű adatokkal, vagy közérdekből nyilvános adatokkal kapcsolatos iratok megismerését, iratokba történő betekintést, valamint a másolatok készítésének lehetőségét.

c) belépést azokba a helységekbe, ahol az adatkezelés folyik, illetetve hozzáférést az adatkezelési műveletek végzéséhez használt eszközökhöz

43. Amennyiben az Intézet a Hatóság adatvédelmi és titokfelügyeleti hatósági eljárásban hozott határozatát nem fogadja el, adatvédelmi hatósági eljárás esetén az adatvédelmi tisztviselő, titokfelügyeleti hatósági eljárás tekintetében a biztonsági vezető véleményezését követően a bírósági felülvizsgálat kezdeményezésére a nyitva álló határidőn belül a bírósághoz fordulhat. A bíróság jogerős döntéséig a vitatott adatkezelésben érintett adatok nem semmisíthetők meg, illetve nem törölhetők.

6. Adatvédelmi előírások betartásának ellenőrzése

44. Az Intézetre vonatkozó adatkezelési szabályok betartásának ellenőrzésére jogosult, a parancsnok, adatvédelmi tisztviselő, BVOP. ellenőrzési szolgálatának és Jogi és adatkezelési főosztály felhatalmazott tagja, a belügyminisztérium által írásban felhatalmazott személy, valamint a jogszabályban felhatalmazott személyek.

45. Az ellenőrzést végző személy részére biztosítani kell a belépést azon helységekbe, ahol az adatkezelés folyik, illetve a felvilágosítás kérésének lehetőségét az adatkezelést végző személyektől.

46. Az ellenőrzés végrehajtó személy jogosult az Intézet adatkezelési tevékenységével összefüggő adatkezeléseket megismerheti, illetve betekinteni azokba, amennyiben az adatok megismerését jogszabály nem korlátozza.

7. Személyállomány oktatása, illetve tájékoztatása

47. Az Intézet személyállományába újonnan felvételre kerülő, adatkezelési feladatokat ellátó személyt az állományba vételétől számított négy hónapon belül az adatvédelmi tisztviselő kioktatja az adatvédelmi előírásokról, valamint rendelkezésére bocsájtja a szükséges szabályozókat. A személyállomány tagjának adatvédelmi szabályokkal kapcsolatos oktatását, közvetlen elöljárója írásban kezdeményezi az adatvédelmi tisztviselőnél, aki az oktatás végrehajtásáról jegyzőkönyvet készít.

48. Az adatvédelmi tárgyú jogszabályokban, a közérdekű adatok nyilvánosságával kapcsolatos jogszabályokban, illetve normákban bekövetkezett változás esetén az adatvédelmi tisztviselő köteles tájékoztatni az adatkezelést végrehajtó állományt.

49. Amennyiben a jogszabályokban, illetve normákban különösen jelentős mértékű változás következik be, amely indokolttá teszi a személyállomány képzését, az adatvédelmi tisztviselő a változásról jelentést tesz az intézet parancsnok részére, illetve kezdeményezi a személyállomány oktatásának végrehajtását.

8. Védelmi intézkedések

50. Az 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.

51. A személyes adatok védelme érdekében a személyes, vagy különleges adatokat tartalmazó iratokat, illetve adathordozókat arra rendszeresített, páncélszekrényben, vagy biztonsági zárral és szárazlakattal ellátott lemezszekrényben, vagy biztonsági zárral, vasráccsal és szárazlakattal, illetve elektronikus védelemmel ellátott helységben kell elhelyezni.

52. 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.

53. A helységek kulcsdobozát 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.

54. 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.

55. A személyi állomány tagjai a munkaköri vagy szolgálati feladatuk ellátáshoz szükséges adatbázisokhoz és nyilvántartásokhoz hozzáféréséhez történő jogosultságot a szakterületi vezető személyre szabottan állapít meg. A jogosultság, illetve annak mértékét a személyállományi tag munkaköri leírásában kell rögzíteni. A jogosultság megállapítására alapot adó körülményekben változás történik, a szakterületi vezető haladéktalanul intézkedni köteles a jogosultság módosításra vagy visszavonására.

56. Az esetlegesen az adatkezelők körében bekövetkezett személyi változások tekintetében, a betekintési illetve hozzáférési jogosultságot meghatározó elöljáró haladéktalanul köteles intézkedni a jogosultság visszavonására.

57. Személyállományi tag szolgálati jogviszonyának megszűnése esetén, a betekintési illetve hozzáférési jogosultságot legkésőbb az állományban töltött utolsó napon vissza kell vonni. A személyállományi tag leszerelő lapja csak abban az esetben írható alá, amennyiben jogosultság visszavonásának ténye rögzítésre került azon.

58. Az elektronikus információs rendszerben keletkezett, továbbított, illetve feldolgozott személyes adatok adminisztratív, fizikai és logikai védelmét biztosítani kell.

a) Az adminisztratív védelem biztosítása érdekében az informatikai csoportvezetőnek (GEI) gondoskodni kell az ellenőrzési, intézkedési és szabályozási kötelezettségek megtételéről, valamint a védelmi intézkedések oktatásáról.

b) A fizikai védelem biztosítása érdekében biztosítani kell a rendelkezésre állás és működőképesség megőrizhetőségének követelményeit. Az Intézet által használt hardver eszközöket kategorizálását végre kell hajtani, a feldolgozott, keletkezett és továbbított kategóriáknak megfelelően. A hardvereszközök védelme esetén kiemelt figyelmet kell fordítani azok érzékenységére, valamint a tárolt adatok magas fokú rendelkezésre állására. A kategorizálás végrehajtása, valamint folyamatos felülvizsgálata az informatikai osztály állandó feladata.

c) A logikai védelem során biztosítani kell az adatok bizalmasságát és sérthetetlenségét, amelyhez figyelembe kell venni az érintett adatok érzékenységét.

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

60. Telefonon történő, továbbá személyes megkeresés esetén személyes adatot kiadni tilos, csak hivatalos írásbeli megkeresés alapján, az adatvédelmi jogszabálynak megfelelően, dokumentálva engedélyezett.

61. 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.

62. A munkavégzés során keletkezett rontott vagy fel nem használt személyes adatokat tartalmazó adathordozókat meg kell semmisíteni. Az adathordozók megsemmisítést oly módon kell végrehajtani, hogy abból adat ne legyen kinyerhető.

9. A személyes adatok veszélyhelyzetben történő védelme

63. Rendkívüli esemény, veszélyhelyzet, katasztrófahelyzet esetén, illetőleg következményeinek az elhárítása során a kár elhárítására feladat- és hatáskörrel rendelkező szervek, valamint a biztonsági vezető és adatvédelmi tisztviselő 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.

64. 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 és a biztonsági osztályvezető együtt köteles gondoskodni.

65. Az adathordozók szállítási módját minden esetben az adatvédelmi tisztviselő és az érintett szakterületi vezető közösen határozza meg, oly módon, hogy az adatokhoz illetéktelenek ne férhessenek hozzá.

66. A kár elhárítása után a szakterületi vezetők kötelesek felmérni, hogy történt-e adatvesztés. A felmérés eredményéről a szakterületi vezető tájékoztatja az adatvédelmi tisztviselőt és jelentést tesz az intézet parancsnoka részére.

10. Kamerahasználat

67. 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 csoportvezető (GEI) felel.

68. A kameraképek archiválása során – a Bv. Kódex 150. §-ában foglaltaknak megfelelően – a vonatkozó 25/2025 (XI. 20.) BVOP utasításban foglaltaknak alapján kell eljárni. A rendszerben tárolt adatok archiválása csak parancsnoki engedéllyel lehetséges. Az archiválás végrehajtásáért az informatikai csoportvezető (GEI) a felelős.

69. 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 műszaki és ellátási osztályvezető a felelős.

III. ZÁRÓ RENDELKEZÉSEK

70. Jelen szabályzat a kiadást követő napon lép hatályba. Ezzel egyidejűleg a tárgyban kiadott 30519-3/3-1/2026.int. számú intézkedés hatályát veszíti.

71. Az ellenőrzési nyomvonalat az 5. melléklet tartalmazza.

72. Az intézkedést az érintett személyi állománnyal teljes terjedelemben, dokumentáltan ismertetni kell.

Takács László bv. alezredes
parancsnok

ZÁRADÉK

A dokumentum elektronikus aláírással hitelesített

30519-3/75-1/2026.int.