HADMÉRNÖK

XIII. Évfolyam 1. szám – 2018. március

ADATOK VÉDELME A BÖRTÖNÖKBEN

DATA PROTECTION IN PRISONS

KONDÁS Katalin

(ORCID: 0000-0002-3775-4653)

kondas.katalin@bv.gov.hu

Absztrakt

Az új adatvédelmi törvény, új szabályozókat követel. Az adatvédelem minden szakterületen kiemelkedően fontos. Nincs ez másképp a börtönök mindennapjaiban sem. Az adatokat feldolgozó személyeknek feltétlenül meg kell ismerni az adatvédelemmel kapcsolatos jogszabályokat, a hozzáféréseik fontosságát.
Az informatikai rendszer üzemeltetése során nagymértékű figyelmet kell fordítani az adatok sértetlenségére, ezzel együtt a felhasználók jogosultságainak karbantartására.
A cél egy tudatos felhasználókkal rendelkező rendszer kialakítása. Cikkemben összefoglalom, mely speciális adatvédelemmel kapcsolatos szabályokat szükséges ismerni a börtönökben. Feltárom a visszatérő felhasználói hibákat, illetve javaslatot teszek annak javítására.

Kulcsszavak: *adatvédelem, személyes adat, jogosultság, informatika*

Abstract

The new Data Protection Law, following the new regulators. Data protection is extremely important in any field. It is no different either in prisons every day. The data processing person must be recognized in legislation on data protection, the importance of access.
During the operation of large-scale IT systems attention to data integrity, along with the maintenance of rights of users.
The aim is to create a system-conscious user with. I summarize my article, which is necessary to know the rules on data protection in special prisons.
I reveal the return of user errors, or propose to do to improve.

Keywords: *data protection, personal data, permission, IT*

A kézirat benyújtásának dátuma (Date of the submission): 2017.11.22.
A kézirat elfogadásának dátuma (Date of the acceptance): 2018.03.18.

BEVEZETÉS

2016. májusában kihirdették az EU Általános Adatvédelmi Rendeletét (angolul: General Data Protection Regulation, rövidítve: GDPR, a továbbiakban: Rendelet), amelynek pontos megnevezése az Európai Parlament és a Tanács (EU) 2016/679 Rendelete (2016. április 27.) természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) lett. A Rendelet hatályba lépésének ideje nem egyezik az alkalmazásának időpontjával. Az új európai adatvédelmi rendeletnek 2018. május 25-től kell megfelelni, és azt kötelezően alkalmazni egész Európában. A rendelkezésre álló két év soknak tűnhet, azonban ebben az időszakban kell a tagállamoknak minden törvényt, szabályt, előírást módosítani úgy, hogy azok a rendeletben megfogalmazott adatvédelmi szabályoknak megfeleljenek. [1]

Magyarországon folyamatban van a jelenlegi jogszabályi háttér átvizsgálása, kialakítása a Rendelet előírásainak megfelelően. Az elmúlt egy évben folyamatosan zajlik a Rendelet rendelkezéseinek való megfelelésre felkészülés. Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) jelenleg is tartalmazza azt a szabályt, miszerint bizonyos adatok kezelése csak úgy lehetséges, ha ahhoz a természetes személy előzetesen hozzájárul. Ebbe a körbe ezután a biometrikus és a genetikai adatok is besorolhatóak. [2]

Az Alaptörvény VI. cikk (2) bekezdése szerint „Mindenkinek joga van személyes adatai védelméhez…” [3] Az Infotv. a következőképpen határozza meg a személyes adat fogalmát: „az érintettel kapcsolatba hozható adat - különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret -, valamint az adatból levonható, az érintettre vonatkozó következtetés”. [2]

A büntetés-végrehajtásban a személyes adatok védelme nemcsak a személyi állományra, hanem természetesen a fogvatartottakra is kiterjed. A büntetés-végrehajtási jogviszony jellegéből eredően a büntetések végrehajtása során a fogvatartottat jogszabályban meghatározott sajátos jogok és kötelezettségek illetik meg. Az Alaptörvényben meghatározott alapvető jogokat, a határozatában meghatározott korlátozásokkal vagy tilalmakkal, a büntetés-végrehajtás rendjével összhangban gyakorolja. [4]

A büntetés-végrehajtásnál kezelt információkhoz tartozik mind a személyi-, mind a fogvatartotti állománnyal kapcsolatos személyes adatok. Ezek kezelése, tárolása elektronikusan az informatikai rendszerben történik, ennek értelmében az informatikai rendszer elemeinek védelme a legfontosabb feladat. [5; 594-595.] Publikációm célja a szervezetnél rögzített, tárolt, módosított, törölt adatok jelenlegi informatikai védelmének feltérképezése, vizsgálata az arra jogosultak tekintetében, a jogszabályi háttér áttekintése, az informatikai rendszer hozzáférések szabályozottságának elemzése. Célom a rendelet által előírt változások vonatkozásában új javaslatok kidolgozása a hatékonyabb jogosultság kiosztásban, ellenőrzésében az adatok védelmének növelése érdekében.

BELSŐ SZABÁLYOZÓK

A személyes információ, illetve a személyes adat védelmének szükségessége kiemelkedő az adatvédelmi rendelet előírása alapján.

A büntetés-végrehajtási szervezet (a továbbiakban: bv. szervezet) működése szempontjából az alábbi egységekre sorolható, melyek együttes elnevezése a bv. szervek:

- Büntetés-végrehajtás Országos Parancsnoksága (a továbbiakban: BVOP)
- Büntetés-végrehajtási intézmények
- Büntetés-végrehajtási intézetek
- Gazdasági társaságok.

A BVOP a bv. szervezet középirányító szerve. Felügyeli, ellenőrzi és szakmailag irányítja a büntetés-végrehajtási intézetek, intézmények, és a gazdasági társaságok szolgálati feladatainak a végrehajtását, így különösen a fogvatartás biztonságával, a fogvatartottak reintegrációjával, foglalkoztatásával, egészségügyi ellátásával, szállításával és nyilvántartásával, valamint a büntetés-végrehajtási pártfogó felügyelői tevékenység ellátásával kapcsolatos feladatokat. A büntetés-végrehajtási intézmények a személyi állomány oktatását, rehabilitációját, valamint a fogvatartottak egészségügyi ellátását és a kényszergyógykezelés végrehajtását szolgáló intézmények. A *büntetés-végrehajtási intézetek*: a fogvatartottak elhelyezésére létesült objektumok. A gazdasági társaságok a fogvatartottak foglalkoztatására létrehozott gazdálkodó szervezetek, tevékenységük során az értékteremtő munkát, a társadalmilag hasznos tevékenységet helyezik a középpontba.

A bv. szervezet az egységes feladat végrehajtás érdekében belső szabályozókat hoz létre, mely tartalma alapján lehet utasítás, illetve szakutasítás, jogszabállyal vagy közjogi szervezetszabályozó eszközzel ellentétes rendelkezést nem tartalmazhatnak. Az utasítás a bv. szerv tevékenységére, működésére vonatkozó előírás, a személyi állomány egészét érintő feladatok meghatározására szolgál, kiadására kizárólag az országos parancsnok jogosult. Ezzel szemben a szakutasítás a szakirányítási feladatok olyan szabályozási eszköze, mely a bv. szervek mindennapi tevékenységének általános, technikai jellegű rendezést igénylő kérdéseire adható ki. [6] Minden intézet - működésének sajátosságait figyelembe véve, - a szakutasítások betartása mellett helyi parancsnoki intézkedéseket adhat ki.

A bv. szervezet az új adatvédelmi rendeletet, és az információs önrendelkezési jogról és az információszabadságról szóló törvény tartalmaira figyelemmel ebben az évben egy Adatvédelmi és Adatbiztonsági Szabályzatot adott ki. A szakutasítás hatálya a bv. szerv teljes személyi állományát annak betartására kötelezi.

A szakutasítás kibocsátásának célja, hogy a bv. szervek tevékenységük során a személyes adatok védelméhez fűződő alkotmányos alapjogon alapuló információs önrendelkezési jog érvényesülését biztosítsák, illetve az általuk kezelt személyes adatok jogosulatlan felhasználásának megakadályozása érdekében meghatározásra kerüljenek az adatvédelmi és adatbiztonsági előírások. Kiterjed a bv. szervek kezelésében lévő közérdekű adatok megismerésére irányuló igények elbírálására, valamint az elektronikus formában közzéteendő adatok nyilvánosságra hozatalával összefüggő feladatok meghatározására egyaránt. A szakutasítás meghatározza egy adatvédelmi tisztviselő kinevezését, aminek célja az adatbiztonság megerősítése, és az érintettek jogérvényesítésének elősegítése. [7]

AZ ADATVÉDELEM INFORMATIKAI VONATKOZÁSAI

Az informatikai rendszer üzemeltetése során feladatként jelenik meg az információk folyamatos rendelkezésre állásának biztosítása, valamint az adatok illetéktelen hozzáféréstől való védelme. A speciális adatok kezelésének, felhasználásának egyik alapvető nyomon követhetősége érdekében a felhasználók azonosítása és az információk hitelesítési folyamatának kialakítása jelentős fontosságú.

A büntetés-végrehajtás Informatikai Biztonsági Szabályzatának (a továbbiakban: IBSZ) alapvető célja, hogy az informatikai rendszer alkalmazása során biztosítsa az információk védelmét, megakadályozza az adatokhoz történő jogosulatlan hozzáférést. A rendszerben kezelt adatok bizalmassága, hitelessége, sértetlensége és rendelkezésre állása alapvető követelmény, funkcionalitás szempontjából folytonosnak és teljes körűnek kell lenni. [8]

Az elektronikus adatok védelme függ az informatikai rendszer fizikai kialakítástól, a személyi hozzáférés szabályozottságától, az adatok kezelésétől, és az adatokhoz kapcsolódó egyéb védelmi intézkedésektől. Az adatok védelmének szempontjából a felhasználói jogosultságok kiosztására helyeztem a hangsúlyt. Kutatást végeztem a börtönökben, hogy

milyen feltételek, előírások, engedélyek, dokumentumok szükségesek az rendszerben szereplő adatok hozzáféréshez.

Az új általános adatvédelmi rendelet elsősorban a személyes adatok kezelését hivatott szigorúbb keretek közé terelni. A bv. szervezetnél ide tartozik a személyi- és a fogvatartotti állománnyal kapcsolatos minden információ. A bv. a következő nyilvántartásokat vezeti, amelyek személyes adatokat tartalmaznak:

- személyügyi nyilvántartás,
- fegyelmi- és büntető ügyek nyilvántartása,
- szolgálatszervezés,
- személyi állomány kiértesítéséhez, riadóztatásához szükséges adatok nyilvántartása,
- illetményszámfejtés,
- elszámolással kapcsolatos nyilvántartások (pl. túlszolgálat, pótlékok, költségtérítések, kiküldetés),
- cafetéria,
- ruházati ellátás,
- lövészeti és fizikai állapot felmérés nyilvántartások,
- informatikai szakterület által vezetett nyilvántartások (pl.: informatikai felhasználói azonosítók, telefonáláshoz kapcsolódó kódok),
- biztonsági intézkedésekkel összefüggő adatkezelések,
- munkabalesetek,
- személyi állomány egészségügyi ellátásáról vezetett nyilvántartások,
- fogvatartottak egészségügyi ellátásáról vezetett nyilvántartások,
- fogvatartottak nyilvántartása,
- fogvatartotti letét,
- fogvatartottak kapcsolattartási, telefonálási adatai,
- fogvatartottak munkáltatásával kapcsolatos adatok, munkadíj számfejtésének adatai,
- egyéb, jogszabály által előírt nyilvántartások. [6]

Az 1. számú táblázat pontosan tartalmazza, hogy 2017. július 7. napján pontosan hány aktív személy szerepel a nyilvántartásunkban. A már leszerelt, eltávozott munkatársakat és fogvatartottakat nem tartalmazza a statisztika.

Bv. szervek létszáma	
Állomány	**Fő**
Alkalmazotti	8.945
Fogvatartotti	17.918
Összesen	**26.863**

1. táblázat A bv.-nél nyilvántartott, aktív személyek száma (saját szerkesztés)

A bv. szervezet informatikai rendszeréhez a jelenlegi alkalmazotti állomány minden tagja rendelkezik valamilyen szintű hozzáféréssel. A szervezet fő alkalmazásai a személyügyi-, és a fogvatartotti nyilvántartó rendszer, amelyek a büntetés-végrehajtás állomány személyes adatait tartalmazza. A rendszerek működésének alapja, hogy a BVOP-n helyezkednek el mind

a központi adatbázisok, mind a központi alkalmazás szerverek. Minden intézetben megtalálható az intézeti adatbázis szerver, amely a központi adatbázis adatait tartalmazza folyamatosan frissülő másolatban, illetve az intézeti alkalmazás szerver. Normál működés esetén az egyes felhasználók a hozzájuk rendelt intézeti vagy központi alkalmazás szerveren keresztül érik el a központi adatbázist. Minden felhasználó a központi adatbázisban tárolt adatokat kezeli, a jogosultsági rendszerben szabályozott módon. Abban az esetben, ha az egyes komponensek közötti kapcsolat megszakad, a munkaállomások az alkalmazás szervereken keresztül a lokális adatbázis másolatot használják. A kapcsolat helyreállása után a helyben végzett adatrögzítések és módosítások visszakerülnek a központi adatbázisba.

JOGOSULTSÁGOK SZEREPE

Az Infotv. szerint az

- „adatkezelő: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely önállóan vagy másokkal együtt az adat kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja”,
- „adatfeldolgozó: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely szerződés alapján - beleértve a jogszabály rendelkezése alapján kötött szerződést is - adatok feldolgozását végzi”. [2]

Az informatikai rendszerben szereplő adatok biztonságát több tényező is befolyásolja. Ezek közül legfontosabb, hogy a felhasználó személye azonosítva legyen annak érdekében, hogy csak azokhoz az információkhoz férjen hozzá, amelyekhez jogosultsággal rendelkezik. Ezáltal az illetéktelen hozzáféréseket korlátozni tudjuk. [9]

Az előző fejezetben említett alkalmazásokban az egyes felhasználók által elvégezhető műveleteket a jogosultsági rendszer szabályozza. Minden felhasználó egy vagy több ún. szerepkörbe van sorolva. Ezen szerepkörök határozzák meg, hogy az egyes felhasználók milyen funkciókat érhetnek el, adatokat láthatnak a rendszerben. A munkakör, illetve a szolgálati feladatok határozzák meg, hogy melyik felhasználónak milyen szerepkörhöz tartozó hozzáférés szükséges az egyes alkalmazások használatához. A jelenlegi szerepkörök és funkciók összerendelését jogosultsági mátrixok tartalmazzák, ezt szemlélteti az 2. táblázat. Az következő táblázatokban a rendszeresített fogvatartotti nyilvántartó rendszer egyik moduljának jogosultsági rendszere látható: a feladatok egy-egy elkülönült jogosultságként jelennek meg, és munkakörhöz kötöttek. A 3. táblázat szemlélteti az informatikai jogosultság elnevezését. A nyilvántartó rendszer folyamatos fejlesztés alatt áll, a modulok száma is növekszik, a szerepkörök száma jelenleg meghaladja a 100-at.

	Program menüpont megnevezése	Kártyakészítő	Nevelő	Fényképező	Adatmegtekintő
1	Fényképezések listázása		X	X	X
2	Fogvatartotti kártyák listázása	X	X		X
3	Fényképek megtekintése		X	X	X
4	Új fényképek rögzítése			X	
5	Összes fogvatartotti fénykép törlése			X	
6	Új kártya készítése	X			
7	Kártya adatainak megtekintése	X	X		X
8	Kártya letiltása	X	X		
9	Kártya nyomtatása	X			

2. táblázat Jogosultsági mátrix (saját szerkesztés)

Csoportok
kartyakeszito
nevelo
fenykepezo
adatmegtek

3. táblázat Szerepkörök (saját szerkesztés)

A szervezet informatikai rendszerében tárolt személyes adatok kezelése során tehát biztosítani kell a betekintési jogosultság megfelelő korlátozását, terjesztését és megismerését biztosító szerepkör alapú differenciált hozzáférést. Ilyen adatok csak törvényben meghatározott célból, a feladat végrehajtásához szükséges mértékben kezelhetők. Az adatkezelés teljes életciklusában biztosítani kell ezeknek a követelményeknek érvényesülését. Korlátozott terjesztésű adatok kezelését úgy kell megvalósítani, hogy az adatokba való betekintés illetéktelen személy által képernyőn, eredmény listán se valósulhasson meg. [8]

Informatikai szolgáltatások, alkalmazások igénybevételéhez, a felhasználó feladatainak végrehajtásához szükséges a jogosultsági szint megjelölése mellett, hogy az aláírásával és a közvetlen vezető jóváhagyásával dokumentáltan kérje azt a helyi informatikai szervezeti egység felé. Az alkalmazotti-, illetve a fogvatartotti adatnyilvántartó rendszerekhez való hozzáféréshez szükséges az adatgazda szakterület egység vezetőjének engedélye is. A kiosztott jogosultságok ezáltal visszakereshetővé válnak és nyomon követhető, hogy azokat ki engedélyezte.

A felhasználói azonosítás során a helyes jelszókezelés elengedhetetlen, a rendszer 90 naponta kikényszeríti annak változtatását. A jelszavak minimális hossza, összetétele, lejárati ideje, ismétlődése, elírásának száma, különleges karakterek száma szabályozott, illetve nem választható az előzőleg megadottak egyike sem. A jelszavaknak akkor van jelentősége, ha a felhasználó tisztában van a fontosságával.

TAPASZTALATOK

A jelenlegi jogosultsági mátrix kialakításának alkalmazása a gyakorlatban jól működik. A felhasználók jogosultság kiosztása a vezető, illetve az adatgazda engedélyéhez kötötten, az informatikai rendszergazda feladataként valósul meg. A szerepkörök beállításaiból

megállapítható, hogy a felhasználók mely személyes adatokhoz férnek hozzá, melyeket rögzítik, módosítják, törlik.

A bv. szervezet személyi állományát - szakmai felkészültsége érdekében, - folyamatosan képezni kell. A jogszabályok, belső szabályozók rendszeresen változnak, bővülnek, újak kiadására kerül sor. Ezeket célszerű oktatás keretében évente legalább két alkalommal megismertetni, átismételni a kollégákkal. Az új adatvédelmi rendelet megfelelő alkalmazásához elengedhetetlen annak ismerete. Az adatok védelmének fontosságát folyamatosan tudatosítani kell az adatokkal dolgozó munkatársakban. [10]

A rendszer használata során talán a legfontosabb, hogy a felhasználókban tudatosítsuk: a belépési név-jelszó páros egyedi azonosító, amely a rendszerben történő tevékenységük azonosításával egyenlő. Kötelesség úgy kezelni, hogy ahhoz más – illetéktelen személy – ne férjen hozzá, ne ismerhesse meg. Ha azt tapasztalja, hogy valaki más is ismeri az általa használt jelszót, akkor azt jelezni kell az informatikai szakterület felé, és ezzel egyidejűleg annak megváltoztatását végre kell hajtani. Ez a legegyszerűbb módja, hogy illetéktelenek olyan adatokhoz férjenek hozzá, melyek munkájukhoz nem szükséges. Tapasztalataim alapján megállapítható, hogy a hozzáférésüket átadó felhasználók két nagy csoportba oszthatók az informatikai rendszerünket használók körében: akik tudatosan adják át másoknak a hozzáférési kódjaikat, így bármikor jogosulatlanul használhatják nevükben a rendszert. A másik típus, aki ugyan nem adja át a kódot, de belépése után magára hagyja a számítógépet, és nem vesz tudomást arról, ha esetleg más felhasználó a kódjával tevékenykedik. Természetesen mindkét eset veszélyes, hiszen, ha az ő jogosultságára vezethető vissza bizalmas információ kiszivárgása, adatok rongálása, megsemmisülése, akkor a következményeket neki kell viselnie.

A munkaállomáson végzett feladatok végrehajtása során gondoskodni kell a felhasználó hosszabb inaktivitása során a kikényszerített kijelentkezésről, vagy az eszköz használhatóságának korlátozásáról, pl. jelszavas képernyő védelemmel. A szervezettől tartósan távollevők jogosultságait törölni kell. A távozottakat belépési felhasználóneveikkel együtt szükséges eltávolítani az informatikai rendszerből. [8]

INFORMATIKAI FELADATOK AZ ADATOK VÉDELMÉNEK ÉRDEKÉBEN

Az adatok tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig tegye lehetővé. Az adatkezelést úgy kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága. Az adatok jogosulatlan vagy jogellenes kezelése, véletlen elvesztése, megsemmisítése vagy károsodásával szembeni védelmet biztosítani kell.

A büntetések, az intézkedések, egyes kényszerintézkedések és a szabálysértési elzárás végrehajtásáról szóló 2013. évi CCXL. törvény (a továbbiakban: Bv. kódex) szerint az e törvényben meghatározott feladatai teljesítése céljából a bíróság, az ügyészség és a végrehajtásért felelős szerv a büntetések, az intézkedések, egyes kényszerintézkedések és a szabálysértési elzárás végrehajtására vonatkozó adatokat, továbbá a végrehajtással összefüggésben az elítéltre vagy az egyéb jogcímen fogvatartottra vonatkozó személyes adatokat kezeli. A Bv. kódex megköveteli, hogy a fogvatartotti személyes adatokat a büntetés, az intézkedés, a kényszerintézkedés, vagy a szabálysértési elzárás végrehajtása befejezésekor vagy végrehajthatósága megszűnésekor törölni kell. [4]

A jogosultságok testre szabását célszerű munkakörökhöz csatolt hozzáférésekkel meghatározni. Így az egy munkakörrel rendelkező állományi tagok egyforma beállításokkal rendelkeznének a kiosztása nyomon követhetőbb, átláthatóbb lenne. Megnehezíti azonban ezt a fajta egységes gondolkodást az, hogy mindig vannak egyedi, személyre szabott külön

kérések, melyek a munkakörtől eltérő hozzáférést igényelnek. Így sok esetben az azonos beosztásban dolgozó állományi tagok különböző szerepkörökhöz vannak rendelve.

A bv. szervezet objektumaiban végrehajtott tevékenységébe csak olyan személyeket, vállalkozót von be, akik személyes adataik kezeléséhez, az adatok szerinti ellenőrzésükhöz hozzájárulnak, szükség esetén erkölcsi bizonyítvánnyal igazolják büntetlen előéletüket, és titok- és adatvédelmi nyilatkozatot tesznek.

A jogosultságok ellenőrzésére figyelmet kell fordítani. Az írásos engedélyen szereplő felhasználói hozzáférést rendszeresen célszerű összevetni a beállítottal. Az ellenőrzésnek azért van jelentős szerepe, mivel sok esetben változik a felhasználók beosztása és ezzel együtt az informatikai hozzáférésük is módosul. A folyamatos kontrollhoz azonban szükség van a szakterület humán erőforrására, amely a jelenlegi állomány bővítésével lenne kivitelezhető. Lehetőségként nem utolsó az sem, hogy a hozzáférések kiosztását naplózzuk. Ennek előnye, hogy nemcsak papír alapon, hanem elektronikus úton is vissza tudjuk keresni, mely felhasználó jogosultságát mikor kapta, módosították, illetve törölték.

KÖVETKEZTETÉSEK

Mint minden területen, így az adatvédelemben is: az elvárások mindig előrébb vannak a kialakított védelmi koncepcióknál. Az utóbbi években egyre hangsúlyosabb a személyes adatok védelme. Az informatikai rendszerben tárolt adatokat a hozzáférések megfelelő kialakításával, engedélyezésével, kiosztásával, karbantartásával, ellenőrzésével tudjuk megóvni az illetéktelenektől. Fel kell készülni azonban arra, hogy a jogosultság nem garantálja a biztonságos adatkezelést. A korlátozott hozzáférés is lehetőséget ad a véletlen illetve a szándékos károkozásra.

Az informatikai rendszer használata során még mindig a tudatos felhasználói tevékenység kialakítása a cél a börtönökben. A felhasználókban folyamatosan erősíteni kell az adatvédelem fontosságát, ezzel együtt a rendszer rendellenes használatának következményeit. A bv. IBSZ-t aktualizálni kell az adatvédelmi és adatbiztonsági szabályzatnak megfelelően. A jogosulatlan adatkezelés észlelése esetén annak megszüntetésére fel kell hívni a felhasználó figyelmét. Az illetékes adatvédelmi felelősnek is jelezni kell a problémát, aki indokolt esetben a szolgálati út betartása mellett büntető-, szabálysértési, fegyelmi eljárást vagy egyéb felelősségre vonást kezdeményez.

Az új adatvédelmi rendelet megfelelő alkalmazásához biztosítani kell a szervezeten belüli szakmai felkészültséget, célszerű oktatásokat szervezni a felhasználók részére az új jogszabályok megismerése, és alkalmazása érdekében. Fel kell hívni mindenki figyelmét a személyes adatok védelmére. Tapasztalatok szerint még mindig nem tudatosult a felhasználókban, hogy a hozzáférések egyedi személyhez kötöttek és annak kiadásából bekövetkező visszaélés a jogosultság tulajdonosát terheli.

Az informatikai szakterületnek a jogosultságok kiosztását naprakészen kell biztosítani, ennek érdekében a folyamatos naplózás, ellenőrzés elengedhetetlen feladatként jelenik meg. Az informatikusok létszámát tekintve azonban erre még nem áll készen.

FELHASZNÁLT IRODALOM

[1] *AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE (2016. április 27.) 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* (általános adatvédelmi rendelet) (EGT-vonatkozású szöveg)

[2] *2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (Infotv.)* 2011. július 26.

[3] *Magyarország Alaptörvénye* 2011. április 25.

[4] *2013. évi CCXL. törvény a büntetések, az intézkedések, egyes kényszerintézkedések és a szabálysértési elzárás végrehajtásáról (Bv. kódex)* 2013. december 23.

[5] FARKAS T.; PRISZNYÁK SZ.: *Kormányzati célú infokommunikációs hálózatok: A rendészeti szervek infokommunikációs rendszere,* Hadtudományi Szemle, X. 4. (2017) 583-596. o.

[6] *A büntetés-végrehajtás országos parancsnokának 2/2013.(IX.13.) BVOP utasítása a büntetés-végrehajtási szervezet belső szabályozási tevékenységéről*

[7] *A büntetés-végrehajtás országos parancsnokának 52/2017. (V.31.) OP szakutasítása a büntetés-végrehajtási szervek Adatvédelmi és Adatbiztonsági Szabályzatának kiadásáról*

[8] *A büntetés-végrehajtás országos parancsnokának 9/2016. (II.16.) OP szakutasítása a büntetés-végrehajtási szervezet Informatikai Biztonsági Szabályzatáról*

[9] Dr. KRAUSZ M.: *Összefoglaló az adatvédelmi rendeletről* - Net-jog.hu, https://net-jog.hu/wp-content/uploads/2016/12/%C3%96sszefoglal%C3%B3-az-adatv%C3%A9delmi-rendeletr%C5%91l_Net-jog.hu_.pdf (letöltve: 2017. augusztus 1.)

[10] Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH), https://www.naih.hu/felkeszueles-az-adatvedelmi-rendelet-alkalmazasara.html (letöltve: 2017.07.29.)