Ellenőrzés száma: Pj-4/2019.

JELENTÉS

PILISJÁSZFALU KÖZSÉG ÖNKORMÁNYZATÁNÁL AZ INFORMATIKAI RENDSZER, VALAMINT AZ ADATVÉDELMI ÉS ADATBIZTONSÁGI ELŐÍRÁSOK ELLENŐRZÉSÉNEK TAPASZTALATAIRÓL

Ellenőrzés tárgya: Pilisjászfalu Község Önkormányzat informatikai, információs és kommunikációs rendszere.

Ellenőrzés típusa: Rendszer ellenőrzés

Ellenőrzés célja: annak megállapítása, hogy az Önkormányzat informatikai rendszere megfelel az Önkormányzat működésének, teljesíti az adatvédelmi és adatbiztonsági előírásokat, valamint annak megállapítása, hogy az Önkormányzat kialakította és működteti információs rendszerét, eleget tett az előírt közzétételi és adatszolgáltatási kötelezettségének, biztosította az Info tv-ben előírt megőrzési kötelezettségét, szabályzatait és működését az aktuális adatvédelmi jogszabályoknak megfelelően aktualizálta.

Ellenőrzés módja: Az ellenőrzés kiterjed arra, hogy a Pilisjászfalui Önkormányzat által működtetett informatikai rendszer, valamint Informatikai biztonsági szabályzat a jogszabályoknak megfelel-e, valamint, hogy az adatvédelmi és adatbiztonsági szabályzatokat elkészítették és azok a jogszabályoknak megfelelnek-e.

Ellenőrzés időszaka: aktuális időszak

Jogszabályi felhatalmazás: A költségvetési szervek belső ellenőrzéséről szóló 370/2011. (XII. 31.) Korm. rendelet, a számvitelről szóló 2000. évi C. törvény, a helyi önkormányzatokról szóló 2011. évi CLXXXIX. törvény, az államháztartásról szóló 2011. évi CXCV. törvény, valamint az államháztartásról szóló törvény végrehajtásával kapcsolatos 368/2011. (XII.31.) Korm.rendelet (Ávr).

Ellenőrzést végezte: Bartha Szilvia belső ellenőr

Információt adott: Baranyai Mária könyvelő

Helyszíni ellenőrzés időpontja: 2019. november 15.

Általános alapvetések

Az ellenőrzést a helyi önkormányzatokról szóló 2011. évi CLXXXIX. törvény, az államháztartásról szóló 2011. évi CXCV. törvény, az államháztartásról szóló törvény végrehajtásával kapcsolatos 368/2011. (XII.31.) Korm. rendelet (Ávr.), a közpénzekből nyújtott támogatások átláthatóságáról szóló 2007. évi CLXXXI. törvény (Knyt.) előírásainak megfelelően, az értékelt időszakban történt jogszabályváltozások áttekintésével végeztük. Az ellenőrzés módszereinek alkalmazásánál figyelembe vettük a költségvetési szervek belső ellenőrzéséről szóló 370/2011 (XII. 31.) Korm. rendelet, valamint az Önkormányzat gazdálkodással kapcsolatos belső szabályzatainak előírásait és aktuális rendeleteit.

1. ÁLTALÁNOS MEGÁLLAPÍTÁSOK

Pilisjászfalu Község Önkormányzata a 2013. évi L. törvény 11. § (f) pontjának felhatalmazása alapján elkészítette Informatikai biztonsági szabályzatát. A szabályzat Tinnyével közösen készült, a Pilisjászfalui Közös Önkormányzati Hivatal megbízásából. A szabályzat alapos, átlátható, világos, a jogszabályban foglalt feltételeknek megfelel. Az Önkormányzat eleget tett a 2011. évi CXII. törvény rendelkezéseinek és az I. számú mellékletben található közzétételi listában foglaltakat közzétette. Az Önkormányzat információbiztonsági eljárásai szabályozottak ugyan, azonban azokat a gyakorlatban nem alkalmazzák.

Az Önkormányzat kitöltötte, majd rendelkezésünkre bocsátotta a vizsgálathoz szükséges, általunk elkészített informatikai kérdőívet.

A Hivatal az ellenőrzés rendelkezésére bocsátotta az informatikai vizsgálat tárgyát képező anyagokat, azokban hiányosságokat nem tapasztaltunk. Az információs és kommunikációs rendszer felméréséhez azonban az anyagokat nem tudták rendelkezésünkre bocsátani, tekintettel arra, hogy azokat az Önkormányzat nem készítette el.

2. RÉSZLETES MEGÁLLAPÍTÁSOK

2.1. Kockázatelemzés

Az ellenőrzés a vonatkozó hatályos jogszabályok, a Pénzügyminisztérium és az Állami Számvevőszék módszertani ajánlásai, valamint az érvényes belső szabályzatok alapján értékelte a vizsgálatra kerülő folyamat kockázatait.

Megállapítottuk, hogy az Önkormányzat elkészítette Informatikai biztonsági szabályzatát, mellyel megfelelt a 2013. évi L. törvény 11. § (f) pontjának, mely szerint a szervezet vezetője köteles gondoskodni az informatikai szabályzatról.

Pilisjászfalu Község Önkormányzata eleget tett a 2011. évi CXII. törvény rendelkezéseinek és az I. számú mellékletben található közzétételi listában foglaltakat közzétette.

Megállapítottuk, hogy az információs és kommunikációs rendszer felméréséhez szükséges anyagok nem készültek el, így azokat ellenőrizni nem állt módunkban.

2019. nyarán Pilisjászfalu Önkormányzata csődhelyzetbe került, adósságrendezési eljárást kezdeményeztek, csődgondnok került kinevezésre.

Előzőek figyelembe vételével megállapítottuk, hogy a vizsgálat tárgyára vonatkozóan a folyamat **belső kontroll kockázat minősítése magas.**

A kockázat esetleges bekövetkezése miatt valószínűsíthető kár értéket **magas mértékűre értékeljük,** mivel a megfelelő szabályozottság az Önkormányzatnál nem biztosított.

Előzőek alapján, a vizsgálat tárgyára vonatkozóan Pilisjászfalu Község Önkormányzata **kockázatok összesített mértékét magasnak minősítjük.**

2.2. Az Önkormányzat informatikai rendszerének ellenőrzése

2.2.1. Az Informatikai biztonsági szabályzat vizsgálata

Pilisjászfalu Község Önkormányzata a 2013. évi L. törvény 11. § (f) pontjának felhatalmazása alapján, mely szerint a szervezet vezetője köteles gondoskodni az informatikai szabályzatról, elkészítette Informatikai biztonsági szabályzatát. A szabályzat Tinnyével közösen készült, a Pilisjászfalui Közös Önkormányzati Hivatal megbízásából. A szabályzat első oldalán a hatálybeléptetés dátuma hiányzik, egyebekben a szabályzat egységes szerkezetű, jól követhető, világos. A szabályzat 2.3. pontja alapján a szabályzat annak kiadása napján lép hatályba és a jelenlegi verzió visszavonásáig hatályos, azt a munkavállalók megismerték, melyet aláírásukkal igazoltak.

A *szabályzat 1-4. pontjaiban* található az általános rész, melyben meghatározásra került a szabályzat célja, hatálya, annak kiadása, kezelése és felülvizsgálata során követendő szabályok, valamint a dokumentumvédelem témaköre. Ennek alapján a szabályzatban előírt nyilvántartások elektronikus, illetve papír alapú dokumentumban egyaránt vezethetők a Jegyző erre vonatkozó döntése szerint.

A *szabályzat 5. pontja* tartalmazza az általános adat- és információvédelmi szabályokat. Ennek alapján minden hivatali munkavállaló az adatok védelme érdekében köteles gondoskodni a „Tiszta asztal, tiszta képernyő" elv alkalmazásáról.

A *szabályzat 6. pontja* rendelkezik az információbiztonsági szervezetről, melyben kialakításra kerültek a felelősségi szintek. (jegyző, információbiztonsági felelős, IT üzemeltető, szabályzat hatálya alá tartozók)

A *szabályzat 7. pontja* rendelkezik az elektronikus információs rendszerek biztonságáért felelős személyről. Ezen személy megbízása, kinevezése, illetve szükség esetén megbízásának visszavonása a jegyző feladata és felelőssége. Az Önkormányzatnál ilyen személy kijelölésre nem került.

A *szabályzat 8. pontja* tartalmazza a biztonsági osztályba sorolást. Az Ibtv. és a Vhr. előírásai alapján a Hivatal, mint szervezet elvárt biztonsági szintje: 3, tekintettel arra,

hogy a Hivatal szakfeladatait támogató elektronikus információs rendszert használ, de nem üzemelteti azt, továbbá központi üzemeltetésű és több szervezetre érvényes biztonsági megoldásokkal védett elektronikus információs rendszerek felhasználója, illetve feladatai támogatására más külső szolgáltatót is igénybe vesz.

A *szabályzat 9. pontja* rendelkezik az intézkedési tervről. Ennek alapján a Hivatal a megvalósítandó biztonsági intézkedéseket és azok megvalósításának sorrendjét az elvárt biztonsági szint elérése céljából intézkedési, illetve cselekvési tervben kell, hogy meghatározza.

A *szabályzat 10. pontja* a nyilvántartásokat, *11. pontja* pedig az engedélyezési eljárásokat szabályozza. Az elektronikus információs rendszerek nyilvántartásának, valamint az engedélyezési eljárás dokumentációjának elkészítéséért és megőrzéséért a jegyző vállal felelősséget.

A *szabályzat 12. pontja* a kockázatelemzés szabályrendszerét tartalmazza. Ennek alapján a Pilisjászfalui Közös Önkormányzati Hivatal által használt elektronikus információs rendszerek kockázatelemzései és kockázatkezelési eljárásrendjében kerültek rögzítésre az azzal összefüggő tevékenységek, feladatok és felelősségek. Ilyen eljárásrendet a Hivatal nem bocsátott az ellenőrzés rendelkezésére.

A *szabályzat 13. pontja* szabályozza a rendszer és szolgáltatásbeszerzéseket.

A *14. pont* az ügymenet folytonosságának tervezését részletezi. Ezen pontban került szabályozásra az üzletmenet-folytonossági terv informatikai erőforrás kiesésekre, melyet a szabályzat 8. számú melléklete tartalmaz, az üzletmenet-folytonosságra vonatkozó eljárás (esemény felismerése, jelzése, döntés az erőforrás kiesés kezelésének módjáról, vészhelyzet elhárítása, visszatérés a normál működési folyamathoz), a folyamatos működésre felkészítő képzés, az elektronikus információs rendszer mentései, melyeket a 7. számú melléklet tartalmaz, valamint az elektronikus információs rendszer helyreállítása és újraindítása.

A biztonsági események kezelését *a szabályzat 15. pontja* szabályozza. Ezen belül került szabályozásra a biztonsági események figyelése, jelentése, a segítségnyújtás a biztonsági események kezeléséhez, a biztonsági eseménykezelési terve, valamint a képzés a biztonsági események kezelésére.

A *16. pont* a személybiztonság kérdéskörét szabályozza, mint a személybiztonság feltételei, a Hivatallal szerződéses jogviszonyban álló (külső) szervezetre vonatkozó körülmények, az eljárás jogviszony megszűnésekor, az áthelyezések, átirányítások, kirendelések kezelése, a fegyelmi intézkedések, valamint a viselkedési szabályok az interneten.

A *szabályzat 17. pontja* rendelkezik a tudatosság és képzés szabályozásáról. Itt kerültek meghatározásra a kapcsolattartás az elektronikus információbiztonság jogszabályban meghatározott szervezetrendszerével és az e célt szolgáló ágazati szervezetekkel, a képzési eljárásrend, a biztonság tudatosság képzés szükségessége, a szerepkör vagy feladat alapú képzés szabályai, valamint az ezekre vonatkozó dokumentációk szükségessége. A hivatali munkavállalók a 2. számú melléklet – Megismerési nyilatkozat aláírásával igazolták, hogy az információbiztonsági előírásokat, szabályokat megismerték és azok betartását magukra nézve kötelezőnek ismerik el.

A *szabályzat 18. pontja* szabályozza a fizikai és környezeti védelmet. Ebben a pontban került szabályozásra a fizikai védelmi eljárásrend, a fizikai belépési engedélyek (a 9. számú melléklet tartalmazza a belépésre jogosultak nyilvántartását), a fizikai belépés ellenőrzése, a fizikai hozzáférések felügyelete, a látogatók ellenőrzése, a vészvilágítás, a tűzvédelem, a hőmérséklet és páratartalom ellenőrzése, a víz-, és más csővezetéken szállított anyag okozta kár elleni védelem, a be- és kiszállítók, valamint a karbantartók. A Hivatal bár szabályozza ezeket a környezeti kontrollokat, azonban tűzoltó készüléken kívül mással nem rendelkeznek.

A *19. pont* tartalmazza az általános védelmi intézkedéseket, mint az engedélyezés, az elektronikus információs rendszer kapcsolódásai, valamint a külső kapcsolódásra vonatkozó korlátozásokat.

A *szabályzat 20. pontja* a tervezést, *21. pontja* a biztonsági elemzés szabályait, ezen belül a rendszerbiztonsági tervet, a cselekvési tervet, a személyi biztonságot, a biztonságelemzési eljárásrendet, a biztonsági értékeléseket, valamint a biztonsági teljesítmény mérését szabályozza.

A *szabályzat 22. pontja* a tesztelés, képzés és felügyelet szabályait tartalmazza. Ezen belül szabályozza a tesztelési, képzési és felügyeleti eljárásokat, valamint a sérülékenységi-tesztet.

A *szabályzat 23. pontja* szabályozza a konfigurációkezelést, mint konfigurációkezelési eljárásrend, alapkonfiguráció, a konfigurációváltozások felügyelete (változáskezelés), előzetes tesztelés és megerősítés, biztonsági hatásvizsgálat, konfigurációs beállítások, legszűkebb funkcionalitás, elektromos információs rendszerelem leltár (a nyilvántartásnak minimálisan a 12. számú mellékletben meghatározott tartalommal kell rendelkeznie), a szoftverhasználat korlátozásai, valamint a felhasználók által telepített szoftverek.

A *24-25. pontok* a karbantartásra, valamint az adathordozók védelmére vonatkozó szabályokat tartalmazzák. Itt került szabályozásra az eljárásrend, a hozzáférés, a használat, valamint a törlés kérdése is.

A *szabályzat 26-27. pontjai* szabályozza az azonosítás és hitelesítés, valamint a hozzáférés ellenőrzésének kérdéskörét. Ennek alapján az információbiztonsági felelős jogosult a hozzáférések, illetve felhasználói fiókok kezelésével kapcsolatos beállítások és tevékenységek ellenőrzésére, illetve felülvizsgálati tevékenysége során – minimum éves rendszerességgel – auditálja azt.

A *szabályzat 28. pontja* szabályozza a rendszer- és információsértetlenséget. Itt került meghatározásra az eljárásrend, a hibajavítás teendői, a kártékony kódok elleni védelem feladatai, az elektronikus információs rendszer felügyelete, a biztonsági riasztások esetén elvégzendő feladatok, valamint a kimeneti információ kezelésének és megőrzésének feladatai is.

A *29-30. pontok* szabályozzák a naplózást (naplózási eljárásrend, naplózható események, naplóbejegyzések tartalma, napló tárkapacitás, naplózási hiba kezelése, naplóvizsgálat és jelentéskészítés, időbélyegek, a naplóinformációk védelme, naplóbejegyzések megőrzése, naplógenerálás), valamint a rendszer- és kommunikációvédelem feladatait.

A szabályzatban található eljárásrendeket a Hivatal nem bocsátotta az ellenőrzés rendelkezésére, így azt és annak meglétét nem állt módunkban megvizsgálni.

2.2.2. Az informatikai biztonság gyakorlatának vizsgálata egy, a belső ellenőrzés által készített kérdőív alapján

A vizsgálat tárgyában a belső ellenőrzés készített egy kérdőívet, melyet Pilisjászfalu Község nevében Baranyai Mária könyvelő töltött ki és bocsátott rendelkezésünkre.

A kérdőív *3 témakörrel* foglalkozott, a **szabályozottság vizsgálatával**, a **folyamatos, biztonságos működés feltételeinek ellenőrzésével**, valamint az **üzemeltetés, fejlesztés vizsgálatával**.

A kérdőívből megállapítható, hogy az Önkormányzatnál a gyakorlat hiányos, és az alapos szabályzat ellenére még az alapvető védelmi feladatok sem kerültek meghatározásra.

Nem azonosították és osztályozták a lényeges adatokat és a kritikus folyamatokat, *ugyan meghatározták* az eljárásrendeket az informatikai incidensek esetére, de azokat a gyakorlatban nem alkalmazzák, valamint *nem határozták meg* a szervezeten belül az egyes informatikai folyamatok visszaállítási prioritásait.

Az *adatok és programok mentésére* a megfelelő eljárások kialakításra kerültek, melyeket az Önkormányzat Informatikai Biztonsági Szabályzatának 7. számú mellékletében lévő sablon kitöltésével kellene meghatározni, ez azonban nem történt meg, vagy nem bocsátották az ellenőrzés rendelkezésére. A kérdőív szerint a mentéseket egy előre meghatározott ütemterv alapján, megfelelő gyakorisággal végzik, azonban ennek részletezése nem történt meg. Az adatmentéseket nem tárolják.

A megfelelő környezeti kontroll kialakítása csak részben történt meg, a megfelelő tűzvédelmi berendezések közül tűzoltó készülékkel rendelkeznek, azonban szünetmentes tápegységgel nem rendelkeznek. A személyzet nem megfelelően felkészült a rendkívüli helyzetek kezelésére, a rendszeres továbbképzés nem biztosított.

Nem alakították ki a *hatékony hardver-karbantartási, problémakezelési és változáskezelési eljárásokat*. A hardver karbantartások nem előre ütemezettek, ha meg is történnek annak dokumentálása nem szabályozott. A számítógépes adatfeldolgozási folyamatokat nem a megfelelő rugalmassággal alakították ki ahhoz, hogy mind a megelőző jellegű, mind a váratlan karbantartások, javítások elvégezhetők legyenek. Készenléti hardver eszközök (pl.: háttértárolók, tartalék számítógép, eszközök) nem állnak rendelkezésre. A felmerült problémák összesített elemzésére nem fordítanak figyelmet. A hardver eszközök és szoftverek cseréjét nem egy előre meghatározott terv szerint hajtják végre, amennyiben ez megtörténik.

Az adatfeldolgozásnak és egyéb szolgáltatásoknak a *rendelkezésre állási szintjét* nem határozták meg, és a szabályozottsága sem megoldott. Nem szabályozták le, hogy *az informatikai szervezeti egység milyen szolgáltatási szintet* biztosít a felhasználói rendszerek számára.

Az Önkormányzat az *egyes informatikai üzemeltetési tevékenységek ellátására* külső rendszergazdát vesz igénybe (informatikus végzettséggel). A rendszergazdák és a további külsős cégek felügyelete negyedévente megtörténik, azonban az erre vonatkozó eljárásokat a Hivatal nem részletezte.

A számítógépes hálózati központ egységei, illetve a pénzügyi-gazdálkodási és beszámolási rendszerek *feldolgozási naplókat (ún. log-okat) nem állítanak elő*, azokat a gyakorlatban nem alkalmazzák.

A *felhasználók IT jellegű problémáinak jelentése és kezelése* nem szabályozott, amennyiben egy adott probléma bejelentésre kerül arról összesítés, statisztika nem készül.

Az Önkormányzat *hardvereinek és szoftvereinek konfigurációs nyilvántartását nem vezetik,* a szervezet a konfiguráció-kezelés gyakorlatát nem építette ki.

Az Önkormányzat *nem rendelkezik változáskezelési eljárással*, a specifikációk elkészítése folyamán *nem veszik figyelembe a szoftverek ellenőrizhetőségének követelményét.*

2.2.3. Az Önkormányzat információs és kommunikációs rendszerének felmérése

A Hivatal tájékoztatása szerint a jegyző többszöri kérése ellenére a fenti ügyben semmilyen szabályzat, irat nem készült, így azt ellenőrizni nem állt módunkban.

3. Összefoglalás

Az Önkormányzat eleget tett a 2013. évi L. törvény, valamint a 2011. évi CXII. törvény vonatkozó paragrafusainak és elkészítette Informatikai Biztonsági Szabályzatát. A szabályzat egységes szerkezetű, világos, jól átlátható. Az informatikai rendszerek működése jól szabályozott, az adatvédelem, a kommunikációs biztonság azonban nem megoldott, további intézkedések megtétele szükséges.

4. Javaslatok

1. **Javasoljuk, hogy ahol az általunk készített kérdőívben a válaszuk nemleges volt, azokat a pontokat vizsgálják felül és ennek alapján alakítsák ki az informatikai biztonsági eljárásrendjüket.**

2. **Javasoljuk, hogy az adatvédelemmel, információ biztonsággal (GDPR) kapcsolatos szabályzatokat, iratmintákat, stb. készítsék vagy készíttessék el.**

3. **Javasoljuk Intézkedési terv készítését a fentiekre figyelemmel.**

4. **Javasoljuk továbbá a fenti ügyekben témafelelős kinevezését.**

Budapest, 2019. november 21.

Bartha Gyula
belső ellenőr

1. sz. melléklet a Pj-4/2019. sz. Belső ellenőrzési jelentéshez

TELJESSÉGI NYILATKOZAT

Alulírott ÚJTEGI IZA BELLA HELYETTES JEGYZŐ ....(név, beosztás), büntetőjogi felelősségem tudatában kijelentem, hogy a belső ellenőr részére átadott dokumentumok, legjobb tudásom szerint, mindazon dokumentumok, nyomtatványok, adatok, információk, melyek szükségesek az adott állapot felméréséhez. Kijelentem továbbá, hogy ezek a dokumentumok, adatok és információk megbízható, teljes körű információt tartalmaznak.

Pilisszentiván, 2019. december „ 11 „

az ellenőrzött szervezet vezetője

2. sz. melléklet a Pj-4/2019. sz. Belső ellenőrzési jelentéshez

ZÁRADÉK

Az ellenőrzési jelentés tartalmát megismertem, egy példányát átvettem. A költségvetési szervek belső ellenőrzéséről szóló 370/2011. (XII. 31.) Korm. rendelet értelmében nyilatkozom, hogy

- észrevételt kívánok tenni, és azt a jelentés kézhezvételétől számított 15 munkanapon belül megküldöm a belső ellenőr részére *; (a határidő elmulasztása egyetértést jelent)

- észrevételt nem kívánok tenni*.

Pilisszentiván, 2019. december „ 11 „

az ellenőrzött szervezet vezetője

*a megfelelő szöveget alá kell húzni

** nyilatkoznia kell az ellenőrzött terület, illetve szervezeti egység vezetőjének, illetve annak, akire vonatkozóan a jelentés megállapítást vagy javaslatot tartalmaz,