ÖRVÉNYES KÖZSÉG ÖNKORMÁNYZAT
KÉPVISELŐ-TESTÜLETE
8242 ÖRVÉNYES Fenyves u. 1.
Tel.: 87/ 449 034
onkormanyzat@orvenyes.hu

Iktatószám: 3/369-10/2020.

2020. február 12. Képviselő-testületi ülés
Jegyzőkönyv
9. melléklete

ELŐTERJESZTÉS

Örvényes Község Önkormányzata Képviselő – testületének
2020. február 12. napján tartandó ülésére

Tárgy: Vegyes ügyek – Albacomp Kft.-vel kötött szerződés meghosszabbítása
Előterjesztő: Huszár Zoltán polgármester
Előterjesztést készítette: Németh Tünde jegyző

Tisztelt Képviselő-testület!

2013. július 1-jén lépett hatályba az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Törvény). A jogszabály előírásait az önkormányzatok képviselő-testületének hivatalaira is alkalmazni kellett, így a Tihanyi Közös Önkormányzati Hivatal is érintett.(2. § (1) bekezdés k) pontja)

További kapcsolódó jogszabály az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról szóló 26/2013.(X.21.) KIM rendelet.

A Törvény meghatározza az alapvető információbiztonsági követelményeket:

5. § Az e törvény hatálya alá tartozó elektronikus információs rendszerek teljes életciklusában meg kell valósítani és biztosítani kell

a) az elektronikus információs rendszerben kezelt adatok és információk bizalmassága, sértetlensége és rendelkezésre állása, valamint

b) az elektronikus információs rendszer és elemeinek sértetlensége és rendelkezésre állása

zárt, teljes körű, folytonos és kockázatokkal arányos védelmét.

6. § Az elektronikus információs rendszernek az 5. §-ban meghatározott feltételeknek megfelelő védelme körében a szervezetnek külön jogszabályban előírt logikai, fizikai és adminisztratív védelmi intézkedéseket kell meghatároznia, amelyek támogatják:

a) a megelőzést és a korai figyelmeztetést,

b) az észlelést,

c) a reagálást,

d) a biztonsági események kezelését.

7. § (1) Annak érdekében, hogy az e törvény hatálya alá tartozó elektronikus információs rendszerek, valamint az azokban kezelt adatok védelme a kockázatokkal arányosan biztosítható legyen, az elektronikus információs rendszereket be kell sorolni egy-egy biztonsági osztályba a bizalmasság, a sértetlenség és a rendelkezésre állás szempontjából.

(2) A biztonsági osztályba sorolás alkalmával - az érintett elektronikus információs rendszer vagy az általa kezelt adat bizalmasságának, sértetlenségének vagy rendelkezésre állásának kockázata alapján - 1-től 5-ig számozott fokozatot kell alkalmazni, a számozás emelkedésével párhuzamosan szigorodó védelmi előírásokkal együtt.

(3) A biztonsági osztályba sorolást a szervezet vezetője hagyja jóvá, és felel annak a jogszabályoknak és kockázatoknak való megfelelőségéért, a felhasznált adatok teljességéért és időszerűségéért. A biztonsági osztályba sorolást a szervezet informatikai biztonsági szabályzatában kell rögzíteni.

(4) Az elektronikus információs rendszer bizalmasság, sértetlenség és rendelkezésre állás szerinti biztonsági osztálya alapján kell megvalósítani az 5. és 6. §-ban előírt védelmi intézkedéseket az adott elektronikus információs rendszerre vonatkozóan.

*(5) * A szervezet vezetője az e törvényben meghatározott feltételeknek megfelelő, az elektronikus információs rendszerre irányadó biztonsági osztálynál magasabb, kivételes esetben a hatóság előzetes engedélyével, kockázatokra kiterjedő indoklással ellátva alacsonyabb biztonsági osztályt is megállapíthat az elektronikus információs rendszerre vonatkozóan.*

*(6) * Az európai vagy nemzeti létfontosságú rendszerelemmé a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló törvény alapján kijelölt rendszerelemek elektronikus információs rendszerei tekintetében az e törvényben meghatározott feltételeknek megfelelő, az elektronikus információs rendszerre irányadó biztonsági osztálynál magasabb, a hatóság előzetes engedélyével, kockázatokra kiterjedő indoklással ellátva alacsonyabb biztonsági osztály is megállapítható.*

8. § (1) A biztonsági osztályba sorolást legalább háromévenként vagy szükség esetén soron kívül, dokumentált módon felül kell vizsgálni.....

9. § (1) A kockázatokkal arányos, költséghatékony védelem kialakítása érdekében a szervezetet az elektronikus információs rendszerek védelmére való felkészültsége alapján a szervezetnek biztonsági szintekbe kell sorolni a jogszabályban meghatározott szempontok szerint.

*(2) * Az elektronikus információs rendszer*

a) fejlesztését végző,

b) üzemeltetését végző,

c) üzemeltetéséért felelős vagy

d) információbiztonságáért felelős

szervezeti egységeket az elektronikus információs rendszerek védelmére való felkészültségük alapján a szervezettől elvárt, eltérő biztonsági szintekbe kell sorolni jogszabályban meghatározott szempontok szerint.

*(3) * A szervezet vagy szervezeti egységek biztonsági szintjét a szervezet védelemre való felkészültsége határozza meg.*

*(4) * A szervezet vagy szervezeti egységek biztonsági szintjének meghatározását az elektronikus információs rendszer felhasználásának módja határozza meg, jogszabályban meghatározott szempontok szerint.*

*(5) * A szervezet vagy szervezeti egység az e törvényben meghatározott feltételeknek megfelelő, az adott szervezetre irányadó besorolási szintnél magasabb szintű besorolást is megállapíthat.*

*(6) * Az európai vagy nemzeti létfontosságú rendszerelemmé a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló törvény alapján kijelölt rendszerelemek szervezetei tekintetében az e törvényben meghatározott feltételeknek megfelelő, az adott szervezetre irányadó besorolási szintnél magasabb, vagy indoklással ellátva alacsonyabb szintű besorolás is megállapítható.*

*10. § (1) * A szervezet vagy szervezeti egység jogszabályban meghatározott szempontok alapján meghatározza, hogy a vizsgálat elvégzésekor melyik biztonsági szintnek felel meg.*

*(2) * Ha a vizsgálat alapján meghatározott biztonsági szint alacsonyabb, mint az adott szervezetre vagy szervezeti egységre jogszabályban meghatározott biztonsági szint, akkor a*

szervezetnek a vizsgálatot követő 90 napon belül cselekvési tervet kell készítenie a számára előírt biztonsági szint elérésére.

*(3) * A szervezet vagy a 9. § (2) bekezdése szerinti szervezeti egység biztonsági szintjét a cselekvési tervben szereplő ütemezés szerint kell elérni. Ha a biztonsági szint a vizsgálat alapján az 1. szintet nem éri el, az 1. szint eléréséhez szükséges intézkedéseket az (1) bekezdésben meghatározott szempontok szerint lefolytatott vizsgálatot követő nyolc éven belül meg kell valósítani.*

(4) A 9. § (2) bekezdésében előírt biztonsági szint teljesítése során a szervezetnek lehetősége van az előírt biztonsági szint fokozatos elérésére. Ennek keretében a magasabb biztonsági szint elérésére - minden egyes szintet érintően, a következő magasabb szintre lépéshez - két év áll rendelkezésére.

*(5) * A biztonsági szint meghatározását a 9. § (1) bekezdésében előírt biztonsági szint elérését követően legalább háromévenként, szükség esetén soron kívül, dokumentált módon felül kell vizsgálni.*

*(6) * Az elektronikus információs rendszer biztonságát érintő változás esetén, illetve új elektronikus információs rendszer bevezetésekor a szervezet vagy szervezeti egység biztonsági szintbe sorolását soron kívül meg kell ismételni.*

*(7) * Ha a soron kívüli felülvizsgálat alapján meghatározott biztonsági szint alacsonyabb, mint az adott szervezetre vagy szervezeti egységre előírt biztonsági szint, akkor a szervezetnek vagy szervezeti egységnek a vizsgálatot követő 90 napon belül cselekvési tervet kell készítenie a számára előírt biztonsági szint elérésére.*

*(8) * A szervezet vagy felelős szervezeti egység biztonsági szintbe sorolását a szervezet vezetője hagyja jóvá, és felel annak a jogszabályoknak és kockázatoknak való megfelelőségéért, a felhasznált adatok teljességéért és időszerűségéért. A biztonsági szintbe sorolás eredményét a szervezet informatikai biztonsági szabályzatában vagy szervezeti egységre irányadó szabályzatban kell rögzíteni.*

A Törvény szabályozza, hogy a szervezeteknek az elektronikus információs rendszereik védelmének biztosítása érdekében milyen kötelezettségei vannak, illetve a szervezet vezetőjének – jegyző – milyen feladatai vannak.

11. § (1) A szervezet vezetője köteles gondoskodni az elektronikus információs rendszerek védelméről a következők szerint:

a) biztosítja az elektronikus információs rendszerre irányadó biztonsági osztály tekintetében a jogszabályban meghatározott követelmények teljesülését,

b) biztosítja a szervezetre irányadó biztonsági szint tekintetében a jogszabályban meghatározott követelmények teljesülését,

*c) * az elektronikus információs rendszer biztonságáért felelős személyt nevez ki vagy bíz meg,*

*d)-e) **

f) meghatározza a szervezet elektronikus információs rendszerei védelmének felelőseire, feladataira és az ehhez szükséges hatáskörökre, felhasználókra vonatkozó szabályokat, illetve kiadja az informatikai biztonsági szabályzatot,

g) gondoskodik az elektronikus információs rendszerek védelmi feladatainak és felelősségi köreinek oktatásáról, saját maga és a szervezet munkatársai információbiztonsági ismereteinek szinten tartásáról,

h) rendszeresen végrehajtott biztonsági kockázatelemzések, ellenőrzések, auditok lefolytatása révén meggyőződik arról, hogy a szervezet elektronikus információs rendszereinek biztonsága megfelel-e a jogszabályoknak és a kockázatoknak,

i) gondoskodik az elektronikus információs rendszer eseményeinek nyomon követhetőségéről,

j) biztonsági esemény bekövetkezésekor minden szükséges és rendelkezésére álló erőforrás felhasználásával gondoskodik a biztonsági eseményre történő gyors és hatékony reagálásról, és ezt követően a biztonsági események kezeléséről,

k) ha az elektronikus információs rendszer létrehozásában, üzemeltetésében, auditálásában, karbantartásában vagy javításában közreműködőt vesz igénybe, gondoskodik arról, hogy az e törvényben foglaltak szerződéses kötelemként teljesüljenek,

l) ha a szervezet az adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe, gondoskodik arról, hogy az e törvényben foglaltak szerződéses kötelemként teljesüljenek,

m) felelős az érintetteknek a biztonsági eseményekről és a lehetséges fenyegetésekről történő haladéktalan tájékoztatásáért,

n) megteszi az elektronikus információs rendszer védelme érdekében felmerülő egyéb szükséges intézkedéseket.

(2) Az (1) bekezdésben meghatározott feladatokért a szervezet vezetője az (1) bekezdés k) és l) pontjában meghatározott esetben is felelős, kivéve azokat az esetköröket, amikor jogszabály által kijelölt központosított informatikai és elektronikus hírközlési szolgáltatót, illetve központi adatkezelőt és adatfeldolgozó szolgáltatót kell a szervezetnek igénybe venni.

*(3) * A jogszabály által kijelölt központosított informatikai és elektronikus hírközlési szolgáltató, illetve központi adatkezelő és adatfeldolgozó szolgáltató igénybevétele esetén az (1) és (2) bekezdésben meghatározott feltételek teljesítését a jogszabály által kijelölt központosított informatikai és elektronikus hírközlési szolgáltató, illetve a központi adatkezelő és adatfeldolgozó szolgáltató úgy biztosítja, hogy közreműködik a szervezet és az elektronikus információs rendszer biztonságáért felelős személy feladatai ellátásában a jogkörébe tartozó tevékenységek tekintetében. A két szervezet közötti feladatmegosztást kétoldalú szolgáltatási szerződések biztosítják, amelyek a központi szolgáltató felett felügyeletet gyakorló miniszter vagy megbízottja ellenjegyzésével lépnek hatályba. Az (1) bekezdés a) és b) pontjában meghatározott feladatok keretében a szervezeti szintű informatikai biztonsági szabályok kidolgozása abban az esetben is a szervezet vezetőjének felelőssége, ha a jogszabály által kijelölt központosított elektronikus és hírközlési szolgáltatót vesz igénybe.*

*(4) **

*(5) * A nemzetbiztonsági védelem alá eső állami szervek esetében az elektronikus információs rendszer biztonságáért felelős személy kinevezése tekintetében az eseménykezelő központ előzetes véleményezési jogot gyakorol.*

*(6) * A biztonsági esemény kivizsgálásában részt vevő személy csak az lehet, aki rendelkezik a szervezet vezetője által - az eseménykezelő központ előzetes véleményezésével - kiadott megbízással. A megbízást írásba kell foglalni. A biztonsági esemény kivizsgálásában részt vevő személynek a megbízás előtt részt kell vennie a biztonságiesemény-kezelő eljárásról szóló, eseménykezelő központ által tartott tájékoztató előadáson.*

*(7) * A polgári hírszerző tevékenységet végző nemzetbiztonsági szolgálat elektronikus információs rendszerei, valamint a honvédelmi célú elektronikus információs rendszerek esetében az (5) és (6) bekezdés rendelkezései nem alkalmazhatóak.*

12. § A szervezet vezetője köteles együttműködni a hatósággal. Ennek során:

a) a 11. § (1) bekezdés c) pontjában meghatározott, az elektronikus információs rendszer biztonságáért felelős személyről tájékoztatást nyújt,

b) a szervezet informatikai biztonsági szabályzatát tájékoztatás céljából megküldi,

c) az ellenőrzés lefolytatásához szükséges feltételeket biztosítja
a hatóság részére.

Az elektronikus információs rendszer biztonságáért felelős személy feladatai a Törvény értelmében:

13. § (1) Az elektronikus információs rendszer biztonságáért felelős személy feladata ellátása során a szervezet vezetőjének közvetlenül adhat tájékoztatást, jelentést.

(2) Az elektronikus információs rendszer biztonságáért felelős személy felel a szervezetnél előforduló valamennyi, az elektronikus információs rendszerek védelméhez kapcsolódó feladat ellátásáért. Ennek körében:

a) gondoskodik a szervezet elektronikus információs rendszereinek biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtéséről és fenntartásáról,

b) elvégzi vagy irányítja az a) pont szerinti tevékenységek tervezését, szervezését, koordinálását és ellenőrzését,

c) előkészíti a szervezet elektronikus információs rendszereire vonatkozó informatikai biztonsági szabályzatot,

d) előkészíti a szervezet elektronikus információs rendszereinek biztonsági osztályba sorolását és a szervezet biztonsági szintbe történő besorolását,

e) véleményezi az elektronikus információs rendszerek biztonsága szempontjából a szervezet e tárgykört érintő szabályzatait és szerződéseit,

*f) * kapcsolatot tart a hatósággal és az eseménykezelő központtal.*

(3) Az elektronikus információs rendszer biztonságáért felelős személy e törvény hatálya alá tartozó bármely elektronikus információs rendszerét érintő biztonsági eseményről a jogszabályban meghatározottak szerint tájékoztatni köteles a jogszabályban meghatározott szervet.

(4) Amennyiben a szervezet elektronikus információs rendszereinek mérete vagy biztonsági igényei indokolják, a szervezeten belül elektronikus információbiztonsági szervezeti egység hozható létre, amelyet az elektronikus információs rendszer biztonságáért felelős személy vezet.

(5) Az elektronikus információs rendszer biztonságáért felelős személy biztosítja az e törvényben meghatározott követelmények teljesülését

a) a szervezet valamennyi elektronikus információs rendszerének a tervezésében, fejlesztésében, létrehozásában, üzemeltetésében, auditálásában, vizsgálatában, kockázatelemzésében és kockázatkezelésében, karbantartásában vagy javításában közreműködők,

b) ha a szervezet az adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe, a közreműködők

e törvény hatálya alá tartozó elektronikus információs rendszereit érintő, biztonsággal összefüggő tevékenysége esetén.

(6) Az elektronikus információs rendszer biztonságáért felelős személy e törvény szerinti feladatai és felelőssége az (5) bekezdés szerinti esetekben más személyre nem átruházható.

(7) Az elektronikus információs rendszer biztonságáért felelős személy jogosult az (5) bekezdés szerinti közreműködőktől a biztonsági követelmények teljesülésével kapcsolatban tájékoztatást kérni. Ennek keretében a követelményeknek való megfelelőség alátámasztásához szükséges bekérni a közreműködői tevékenységgel kapcsolatos adatot, illetve az elektronikus információs rendszerek biztonsága tárgyában keletkezett valamennyi dokumentumot.

(8) A szervezetnél csak olyan személy végezheti az elektronikus információs rendszer biztonságáért felelős személy feladatait, aki büntetlen előéletű, rendelkezik a feladatellátáshoz szükséges felsőfokú végzettséggel és szakképzettséggel.

(9) A büntetlen előélet követelményének való megfelelést az elektronikus információs rendszer biztonságáért felelős személy a szervezettel fennálló jogviszonya keletkezését megelőzően köteles igazolni. A szervezet az elektronikus információs rendszer biztonságáért felelős személyt kötelezheti, hogy a szervezettel fennálló jogviszonya alatt a büntetlen előélet követelményének való megfelelést igazolja.

(10) Nem kell a (8) bekezdés szerinti képzettséget megszereznie annak a személynek, aki rendelkezik a külön jogszabályban meghatározott, akkreditált nemzetközi képzettséggel vagy e szakterületen szerzett 5 év szakmai gyakorlattal.

(11) Az elektronikus információs rendszer biztonságáért felelős személy és az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személyek miniszteri rendeletben meghatározott rendszeres szakmai képzésen, továbbképzésen vesznek részt.

2014. évben pályázati eljárás keretén belül kiválasztásra került az ALBACOMP RI Rendszerintegrációs Kft. a feladat ellátására.

A jogszabály szerint kötelező indulási feladatok elvégzésére szerződést kötött a Hivatal 2014. december 31. napjáig, az éves díjat (890.000,- Ft + ÁFA) a Hivatalt alkotó 5 önkormányzat a költségvetésében biztosította.
A költség szétosztása számítógép munkaegységek alapján történt meg.

Az informatikai gépállomány 2014-ben az alábbi volt Örvényesen: 3 db gép.

2014-ben Tihany által fizetendő összeg 327.894,- Ft + ÁFA / év volt.

2014 óta tehát egy új, jogszabály szerint kötelező feladattal bővült a közös hivatalt érintő munkavégzés.
2015-ben a feladatellátásra szerződést kötött a Hivatal további 5 évre, 2015. január 1. napjától 2019. december 31. napjáig összesen 504.000,- Ft + Áfa éves díjért.

Az egyes településekre eső éves bekerülési költség az alábbiak szerint oszlott meg:

Tihany	185.682,- Ft + Áfa
Aszófő	79.578,- Ft + Áfa
Örvényes	**39.789,- Ft + Áfa**
Balatonudvari	92.841,- Ft + Áfa
Balatonakali	106.104,- Ft + Áfa

A Törvény alapján kötelező feladatnak jelen pillanatban is eleget tenni csak egy külső informatikai szervezet útján lehetséges.

Az Albacomp Kft. módosítási kérelmet nyújtott be a Hivatalhoz, melyben a szerződés 5 évvel történő hosszabbítását kérte változatlanul évi 504.000,- Ft + Áfa díjért.

A Pénzügyi és Gazdasági Bizottság megtárgyalta a módosítási kérelmet, és javaslatot tett arra, hogy kizárólag 1 évvel kerüljön meghosszabbításra a szerződés, 2020. december 31. napjáig és az azt követő időszakra újabb pályáztatási eljárás keretében kerüljön kiválasztásra a feladatot ellátó cég.

A Hivatal megkereste az Albacomp Kft-t annak érdekében, hogy nyilatkozzanak, hogy módosítási kérelmüket 1 évvel történő hosszabbítás esetén is fenntartják-e változatlan díj ellenében.

A Kft. - a Bizottság javaslatát figyelembe véve - megküldte új módosítási kérelmét, mely 1 évvel történő határidő hosszabbításról - 2020.12.31. napjáig – szól 504.000,- Ft + Áfa éves díjért.

Az informatikai gépállományban - arányaiban - változás nem történt, így az egyes településekre eső bekerülési költség nem változik.

A fentiek alapján kérem a Tisztelt Képviselőket, hogy az alábbi határozati javaslatot fogadják el:

HATÁROZATI JAVASLAT

Örvényes Község Önkormányzat Képviselő-testületének
...../2020. (.....) határozata

Örvényes Község Önkormányzat képviselő-testülete a Tihanyi Közös Önkormányzati Hivatal elektronikus információbiztonsági követelményeinek az információbiztonságról szóló 2013. évi L. törvényben foglaltak szerinti kötelező biztosítása érdekében felhatalmazza Németh Tünde jegyzőt, hogy az Albacomp Kft (8000 Székesfehérvár, Mártírok útja 9., képviseli: dr. Kertész Ádám ügyvezető) céggel a feladatellátásra megkötött megbízási szerződés módosítását,- mely a 2015. évben aláírt megbízási szerződés 11.3. pontjában meghatározott időtartam 1 évvel, 2020. december 31. napjáig történő módosításáról szól, - aláírja.

A képviselő-testület a feladatellátásból ráeső 37.789,- Ft + Áfa/év összeget a 2020. évi költségvetésében biztosítja és átutalja a Tihanyi Közös Önkormányzati Hivatal számlájára.

Határidő: azonnal.
Felelős: Németh Tünde jegyző

Örvényes, 2020. február 5.

Huszár Zoltán sk.
polgármester