

Ludányhalászi Községi Önkormányzat Polgármestere

Az élet- és vagyonbiztonságot veszélyeztető tömeges megbetegedést okozó világjárvány következményeinek elhárítása, a magyar állampolgárok egészségének és életének megóvása érdekében a Magyarország Kormánya által a veszélyhelyzet kihirdetéséről szóló 27/2021. (I. 29.) Kormányrendeletében elrendelt veszélyhelyzetre tekintettel, a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény 46. § (4) bekezdésében meghatározott jogkörben eljárva, az alábbi határozatot hozom:

Ludányhalászi Községi Önkormányzat Polgármesterének 24/2021. (VI.08.) számú önkormányzati határozata

Ludányhalászi Község Polgármestereként az alábbiakról rendelkezem:

Ludányhalászi Községi Önkormányzat Képviselő-testülete nevében az 1. számú mellékletben foglalt tartalommal elfogadja az önkormányzat 2021. évi belső ellenőrzési jelentést.

A polgármester a döntéséről az érintettet értesíti.

Határidő: értelemszerűen

Felelős: Kovács Imre polgármester

Ludányhalászi, 2021. június 08.



Kovács Imre
polgármester

Szécsény Járási Önkormányzatok Területfejlesztési és Feladatellátási Társulása
Belső ellenőrzés

Iktatószám: *V/263-10*/2021.

ELLENŐRZÉSI JELENTÉS

Ludányhalászi Község Önkormányzat személyes adatok kezelésének rendje

Az ellenőrzést végző neve: Csépe Péter belső ellenőr (belső ellenőri regisztrációs szám: 5112661)

Az ellenőrzés célja: Annak megállapítása, hogy Ludányhalászi Község Önkormányzat a rendelkezésére bocsátott személyes adatokat a jogszabályokban előírtaknak megfelelően kezeli-e.

Az ellenőrzött szervezeti egység: Ludányhalászi Község Önkormányzata

Az ellenőrzés tárgya: Ludányhalászi Község Önkormányzatának személyes adatok kezelésének rendje

Az ellenőrzés típusa: szabályszerűségi ellenőrzés

Az ellenőrzés módszere: jogszabályok és a belső szabályozók alapján dokumentumokon alapuló szűrőpróbaszerű és tételes vizsgálat

Az ellenőrzött időszak: 2020. január. 01 - az ellenőrzési jelentés leadásának időpontjáig.

Jogszabályi és egyéb felhatalmazásra történő hivatkozás:

Az ellenőrzésre a költségvetési szervek belső ellenőrzéséről szóló 370/2011.(XII. 31.) Korm. rendelet alapján, valamint a belső ellenőr 2021. évi ellenőrzési tervében foglaltak figyelembevételével kerül sor.

A belső ellenőrzés során az alábbi fontosabb jogszabályok képezték a munkavégzés alapját:

- 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 (a továbbiakban: Rendelet)
- Magyarország helyi önkormányzatairól szóló 2011. évi CLXXXIX. törvény (Mötv.)
- 370/2011. (XII.31.) Korm. rendelet a költségvetési szervek belső kontrollrendszeréről és belső ellenőrzéséről (Bkr.),
- az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (Ibtv.)
- 41/2015. (VII.15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről
- az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Infotv.)
- a közfeladatot ellátó szervek iratkezelésének általános követelményeiről szóló 335/2005. (XII. 29.) Korm. Rendelet (a továbbiakban IKR),
- a közterület-felügyeletről szóló 1999. évi LXIII. törvény
- a közalkalmazottak jogállásáról szóló 1992. évi XXXIII. törvény (Kjt.)
- a közszolgálati tisztviselőkről szóló 2011. évi CXCV. törvény (Kttv.)
- a szociális ellátásokról szóló 1993. III. törvény (Szocvtv.)
- a gyermekek védelméről és a gyámügyi igazgatásról szóló 1997. évi XXXI. törvény (Gyvt.)
- az anyakönyvi eljárásról szóló 2010. évi I. törvény
- az adózás rendjéről szóló 2017. évi CL. törvény

- a személyi jövedelemadóról szóló 1995. évi CXVII. törvény

I. Általános ellenőrzési megállapítások

Az ellenőrzés célja, annak megállapítása, hogy Ludányhalászi Község Önkormányzata a feladatellátása során a személyes adatok kezelését, tárolását a jogszabályi előírásoknak megfelelően végzi-e. Vizsgálni szükséges a szabályozottság minőségét, teljességét, alkalmazottságát. A cél annak megítélése, hogy a feladatellátás során a személyes adatok kezelése és tárolása a jogszabályi előírásoknak megfelelően történik-e az alkalmazott önkormányzati nyilvántartási rendszerekben.

A vizsgálat során tisztázni szükséges, hogy melyek azok a személyes adatok, amelyeket az önkormányzati feladatellátás egyes területein az ellátások, vagy kötelezettségek megállapításakor szükséges felhasználni, azokat milyen célból kezelik és milyen körülmények között tárolják (elektronikus rendszerek, nyomtatott forma, digitális rögzítés). Fontos vizsgálni, hogy érvényesülnek-e az adatvédelmi alapelvek, a helyi szabályzatok és rendeletek a központi és ez EU jogszabályokkal összhangban kerültek-e megalkotásra.

A GDPR (General Data Protection Regulation) az Európai Parlament és a Tanács (EU) 2016/679 egységes adatvédelmi rendelete, amely 2018. május 25-től kötelezően és közvetlenül alkalmazandó az Európai Unió valamennyi tagállamában, így Magyarországon is. A Rendelet megalkotásának célja, hogy a magánszemélyekre vonatkozó adatok, tranzakciók tárolása és feldolgozása biztonságos keretek között történjen. Az önkormányzatok elektronikus információbiztonságával kapcsolatban a hazai jogalkotás (a 2013. évi L. törvény és a hozzá kapcsolódó 41/2015. (VII. 15.) BM rendelet, valamint 2011. évi CXII. törvény) már korábban is előírásokat fogalmazott meg. Időközben megjelent a 2018. évi XIII. törvény az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény jogharmonizációs célú módosításáról. Az önkormányzati szektor bizonyos értelemben jelenleg szabályozottabbnak és biztonságosabbnak mondható a magyarországi vállalati szektorhoz képest, de a mindenki által ismert problémák (tárgyi és személyi feltételek hiánya) miatt közel sem tökéletes.

A Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: NAIH) iránymutatása alapján az adatvédelmi szabályzat megalkotása a képviselő-testület azon szervét terheli, amely a jogalkotó szerint a kötelezően ellátandó önkormányzati vagy államigazgatási feladat- és hatáskör címzettje. Az önként vállalt feladatok esetén a képviselő-testületnek rendeletben szükséges döntenie az adatkezelő személyéről. Az adatkezelés vagy -feldolgozás jogalapjának meghatározása során a jogszabályon alapuló felhatalmazás ebben a szektorban a legnagyobb, hiszen magát a hatósági munkát és az önkormányzati működést is jogszabályok tömege szabályozza. A GDPR hatálya az önkormányzat intézményeire, gazdasági társaságára is kiterjed, még akkor is, ha utóbbi esetben teljesen mások a kezelendő adatok és azok kezelési módja.

A kapcsolódó szakirodalom szerint az önkormányzati igazgatás egyes területein a GDPR mellett az ASP szakrendszerek bevezetésével is javulni látszott a biztonsági szint, de csak jelentős terhek árán. A kezdeti komolynak mondható nehézségek az idő múlásával ugyan csökkentek, de még mindig nincs meg a megfelelő támogatás a hivatalok, a köztisztviselők részére a szakrendszerek optimális működéséhez. Mindezek mellé megérkezett az elektronikus ügyintézési kötelezettség szinte egy időben, megosztva az önkormányzati tisztviselők figyelmét és erőforrásait.

A GDPR megfelelés kialakításakor abból kell kiindulni – amit a NAIH is mérlegel az ellenőrzései során –, hogy az adatkezelő megtett-e mindent, ami elvárható volt tőle. Azaz a szabályozási és az informatikai környezet megfelelő-e, vagy legalább a megfelelő irányba tart-e a felmérést követően készített intézkedési terv alapján.

A gyakorlatban arra kell törekedni, hogy a megfelelően üzemeltetett információbiztonsági rendszer és jól működő szabályozások mellett a **GDPR megfelelés is kialakításra kerüljön.**

A személyes adatok kezelése során két nagyon fontos dolognak kell megfelelniük az önkormányzatoknak: az alapelveknek, és annak, hogy az adatkezelésnek legyen megfelelő jogalapja.

A vizsgálat szempontjából az önkormányzat a feladatellátása során kezelt személyes adatok zárt rendszerben történő kezelését többnyire szem előtt tartja, és a jogszabályokban előírt kötelezettségeit próbálja betartani. Az információbiztonság területén az önkormányzat rendelkezik Informatikai Biztonsági Szabályzattal és elektronikus információs rendszer biztonságáért felelős személy is kijelölése került, de ezzel még nem teljes körűen megoldott a személyi adatok védelme az adott önkormányzatnál.

Az ellenőrzéshez kapcsolódó általános megállapítások:

A Rendeletben előírt alapelvek érvényesüléséhez és a személyes adatok kezelésének jogszerűségéhez kapcsolódóan az önkormányzat **Adatvédelmi és biztonsági szabályzatának** elkészítése és a felelős kijelölése az ellenőrzés ideje alatt folyamatban volt. A szabályzat hatálya kiterjed az önkormányzatra, a közös hivatalra és az intézményekre, valamint a nemzetiségi önkormányzatra is.

Az információ biztonsági szabályzat tekintetében megállapítható, hogy az önkormányzat rendelkezik szabályzattal és felelős személy is kinevezésre került. A szabályozás és a szakember a jogszabályi előírásoknak és követelményeknek megfelel.

Az Iratkezelési szabályzat megfelel a hatályos jogszabályi előírásoknak, összhangban van az ASP iratkezelési szakrendszerével, az ügyintézők a tartalmát ismerik. Fontos, hogy az önkormányzat az Adatvédelmi és biztonsági szabályzat kidolgozása során az Iratkezelési szabályzatban előírtakat is szem előtt tartsa, valamint a munkaköri leírásokban is rögzítse a kapcsolódó feladatokat.

Ludányhalászi Község Önkormányzatának közigazgatási területén nem kerültek kihelyezésre kamerák. Az önkormányzat épületében, az ügyféltérben nem kerültek kihelyezésre kamerák. Mivel az önkormányzat tulajdonában nincsenek kamerák, kamerarendszert nem működtet, így nincs szükség **kamerarendszer működtetésére vonatkozó szabályzatra.**

Összességében megállapítható, hogy az önkormányzat az adatvédelmi szempontok betartását szem előtt tartja, logikai védelmi eszközöket (jelszavakat) alkalmaz az adatkezelés során a legtöbb információs rendszer használata során.

II. Részletes megállapítások

1. Személyes adatok kezeléséhez kapcsolódó szabályzatok

1.1. Adatvédelmi szabályzat és adatvédelmi tisztviselő

Az Európai Parlament és a Tanács (EU) 2016/679. rendelete kötelezően alkalmazandó az Európai Unió valamennyi tagállamában. A Rendelet a természetes személyeknek a személyes adatok kezelése tekintetében történő védelmére és a személyes adatok szabad áramlására vonatkozó szabályokat állapít meg. A Rendeletet kell alkalmazni a személyes adatoknak az Unióban tevékenységi hellyel rendelkező adatkezelők vagy adatfeldolgozók tevékenységeivel összefüggésben végzett kezelésére, függetlenül attól, hogy az adatkezelés az Unió területén történik vagy nem, valamint ha az adatkezelés az Unióban tartózkodó érintettek személyes adatainak kezelésére irányul, akkor is, ha az Unióban az adatkezelő vagy az adatfeldolgozó tevékenységi hellyel nem rendelkezik.

Az adatkezelőnek, adatfeldolgozónak belső adatvédelmi szabályokat kell alkalmaznia a személyes adatok védelmének biztosítása céljából megvalósított technikai és szervezési intézkedések részeként, ha ez az adatkezelési tevékenység vonatkozásában arányos. A közfeladatot ellátó szerv az Infotv. szerinti kötelezően közzéteendő adatok közzétételi kötelezettségét szabályzat formájú közzétételével teljesíti. A szabályzat célja, hogy a hatálya alá tartozó tárgykörökben az adatok kezelésére vonatkozó alapvető szabályok meghatározása, annak érdekében, hogy a természetes személyek magánszféráját az adatkezelő, munkavállalói vagy egyéb, munkavégzésre irányuló jogviszony alapján foglalkoztatott személyek, illetőleg a szerződéses kapcsolatban álló partnerek vagy más harmadik természetes személyek által tiszteletben tartsák, minden adatkezelési folyamat, munkavégzés, közfeladat teljesítése során a meghatározott adatkezelési célból, a szervezet részére átadott személyes adatainak közlése, továbbítása, feldolgozása, tárolása során biztosítva legyen az adatalanyok információs önrendelkezési jogának maradéktalan érvényesülése, törvényes érdekeinek és jogainak védelme, az adatok kezelésének jogszerű célhoz rendelése és a felhasználás alatt mindvégig e célhoz kötöttsége.

Az adatvédelmi és adatbiztonsági szabályzat további célja, hogy meghatározza a működés során az adatkezeléssel kapcsolatos nyilvántartások vezetésének törvényes rendjét, biztosítsa az adatvédelem alkotmányos alapelveinek, az információs önrendelkezési jognak az érvényesülését, valamint hogy a személyes adatok kezelése a jogszabályokban előírtaknak megfelelően történjen.

Az adatalanyi minőség – és ezáltal az adatvédelmi szabályoknak történő megfelelés követelménye – a személyes adat jogszerű módon történő megszerzésétől kezdődően, az adott jogviszony létrehozásán keresztül annak fennállása alatt és azt követően is fennáll mindaddig, amíg az adott adatalannal összefüggésben a személyes adatok végleges és visszafordíthatatlan módon történő – vagy ahol az lehetséges, illetve szükséges, a megsemmisítése – végrehajtásra nem kerül.

A személyes adatok kezelésére vonatkozóan a jogszabály az alábbi elveket rögzíti:

- jogszerűség, tisztességes eljárás és átláthatóság:** a személyes adatok kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni.
- célhoz kötöttség:** a személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történjen, és azokat ne kezeljék ezekkel a célokkal össze nem egyeztethető módon. Nem

minősül az eredeti céllal össze nem egyeztethetőnek a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból történő további adatkezelés.

3. **adattakarékosság:** a személyes adatok az adatkezelés céljai szempontjából megfelelőek és relevánsnak kell, hogy legyenek, és a szükségesre kell korlátozódniuk.
4. **pontosság:** a személyes adatoknak pontosnak és szükség esetén naprakésznek kell lenniük. Minden ésszerű intézkedést meg kell tenni annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul töröljék, vagy helyesbítsék a műszaki szabályokkal és az információs társadalom szolgálataira vonatkozó szabályokkal kapcsolatos információszolgáltatási eljárás megállapításáról.
5. **korlátozott tárolhatóság:** a személyes adatok tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé; a személyes adatok ennél hosszabb ideig történő tárolására csak akkor kerülhet sor, amennyiben a személyes adatok kezelésére közérdekű archiválás céljából tudományos és történelmi kutatási célból vagy statisztikai célból kerül majd sor, az érintettek jogainak és szabadságainak védelme érdekében előírt megfelelő technikai és szervezési intézkedések végrehajtására is figyelemmel.
6. **integritás és bizalmas jelleg:** a személyes adatok kezelését oly módon kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve.
7. **elszámoltathatóság:** az adatkezelő felelős a fenti alapelveknek való megfeleléséért, továbbá képesnek kell lennie e megfelelés igazolására.

A Rendelet hat lehetséges jogalapot tartalmaz azon személyes adatok kezelésének tekintetében, amelyek nem tartoznak a személyes adatok különleges (pl.: egészségügyi, biometrikus vagy genetikai adatok) kategóriájába. **A személyes adatok kezelése kizárólag akkor és annyiban jogszerű, amennyiben legalább az alábbiak egyike teljesül:**

1. az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez;
2. az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél, vagy az a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges;
3. az adatkezelés az adatkezelőre vonatkozó jogi kötelezettségek teljesítéséhez szükséges;
4. az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges;
5. az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges;
6. az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé, különösen, ha az érintett gyermek.

A Rendeletben előírt alapelvek érvényesüléséhez és a személyes adatok kezelésének jogszerűségéhez kapcsolódóan az önkormányzat Adatvédelmi és biztonsági szabályzatának elkészítése az ellenőrzés ideje alatt folyamatban volt. A szabályzat hatálya kiterjed az önkormányzatra, a közös hivatalra és az intézményekre, valamint a nemzetiségi önkormányzatra is.

Az adatvédelmi szabályzatban kell, hogy rögzítésre kerüljön az **adatvédelmi tisztviselő** személye és elérhetőségei, valamint a személyéhez kapcsolódó feladatok rögzítése is. A költségvetési szerv vezetője felelős azért, hogy az általa vezetett szervezet az adatkezelési, adatfeldolgozási tevékenységét

úgy végezze, hogy megfeleljen a Rendeletnek, felelős azért, hogy az adatkezelési tevékenységek során betartsák a személyes adatok kezelésére vonatkozó elveket, továbbá szükséges, hogy mindezeket igazolni is tudja. Adatvédelmi tisztviselőt minden olyan szervezetnek ki kell neveznie, aki az Infotv. hatálya alá tartozik, vagyis adatkezelő vagy feldolgozó állami feladatot vagy jogszabályban meghatározott egyéb közfeladatot lát el. Az adatvédelmi tisztviselőt a szakmai rátermettsége és különösen az adatvédelmi jog és gyakorlat szakértői szintű ismerete, valamint a Rendeletben az adatvédelmi tisztviselő feladatai között felsorolt feladatok ellátására való alkalmassága alapján kell megbízni.

A Rendelet 39. cikk része rendelkezik az adatvédelmi tisztviselő feladatairól:

„(1) Az adatvédelmi tisztviselő legalább a következő feladatokat ellátja:

- a) tájékoztat és szakmai tanácsot ad az adatkezelő vagy az adatfeldolgozó, továbbá az adatkezelést végző alkalmazottak részére az e rendelet, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezések szerinti kötelezettségeikkel kapcsolatban;
- b) ellenőrzi az e rendeletnek, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezéseknek, továbbá az adatkezelő vagy az adatfeldolgozó személyes adatok védelmével kapcsolatos belső szabályainak való megfelelést, ideértve a feladatkörök kijelölését, az adatkezelési műveletekben vevő személyzet tudatosság-növelését és képzését, valamint a kapcsolódó auditokat is;
- c) kérésre szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, valamint nyomon követi a hatásvizsgálat 35. cikk szerinti elvégzését;
- d) együttműködik a felügyeleti hatósággal; és
- e) az adatkezeléssel összefüggő ügyekben – ideértve a 36. cikkben említett előzetes konzultációt is – kapcsolattartó pontként szolgál a felügyeleti hatóság felé, valamint adott esetben bármely egyéb kérdésben konzultációt folytat vele.

(2) Az adatvédelmi tisztviselő feladatait az adatkezelési műveletekhez fűződő kockázat megfelelő figyelembevételével, az adatkezelés jellegére, hatókörére, körülményére és céljára is tekintettel végzi.”

A Rendeleten túl az Infotv. meghatározza, hogy az adatvédelmi tisztviselő olyan személy lehet, aki „a személyes adatok védelmére vonatkozó jogi előírásokat és jogalkalmazási gyakorlat megfelelő szintű ismeretével rendelkezik és alkalmas a 25/M. § (1) bekezdésében meghatározott feladatok ellátására”.

Összeférhetetlenségi kérdésekről nem rendelkezik az Infotv., itt a Rendelet előírásait kell szem előtt tartani, a következők szerint: 38. cikk (3) bekezdése szerint a tisztviselő jogállását úgy kell kialakítani, hogy senkitől ne fogadhasson el utasításokat a tisztviselői feladatának ellátásával kapcsolatban. A Rendelet 38. cikk (6) bekezdése alapján az adatvédelmi tisztviselő más feladatokat is elláthat, azonban a szervezetnek biztosítania kell, hogy a feladatokból ne fakadjon összeférhetetlenség.

Összességében megállapítható, hogy az önkormányzat vonatkozásában a szabállyal kiadása és felelős személy kijelölése folyamatban van.

1.2. Információbiztonsági Szabályzat

Az állami és önkormányzati szervek, szervezetek vezetői az Ibtv. 11. § (1) bekezdés szerint kötelesek gondoskodni az elektronikus információs rendszerek védelméről, ennek keretében a törvény 11. § (1) bekezdés f) pontja alapján informatikai biztonsági szabályzat elkészítéséről:

„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.”

A Ludányhalászi Közös Önkormányzati Hivatal Informatikai Biztonsági Szabályzata – 2/2018. jegyzői utasítás – 2018. július 1. napjától van érvényben. A szabályzat tartalma megfelel a jogszabályi előírásoknak, időszakos felülvizsgálata esetleg javasolt, de a jogszabályi környezet az elmúlt két évben nem esett át nagyobb változásokon.

A 2020-as év helyzetére tekintettel – a szabályzatban rögzített – két területet célszerű figyelembe venni:

1. oktatás, képzés, tudatosítás

„Cél: folyamatosan gondoskodni arról, hogy a felhasználók tudatában legyenek az informatikai biztonság fenyegetéseinek és motiválva legyenek a szervezet információvédelmi szabályzatainak és intézkedéseinek a betartására. A felhasználók legyenek oktatva a biztonsági eljárásokról és az adatfeldolgozó eszközök helyes használatáról a lehetséges biztonsági kockázatok minimalizálása érdekében.”

A szabályzat hatályba lépésének évében volt informatikai biztonsági oktatás a közös önkormányzati hivatal köztisztviselői részére. Képzés azóta nem volt, ezért célszerű lenne a közeljövőben informatikai biztonsági oktatást szervezni az önkormányzati, közös hivatalok dolgozók részére.

2. távmunka és távoli elérés szabályai

A home office munka engedélyezése, elrendelése előtt szükséges egyeztetni az informatikai biztonsági felelőssel, hiszen a távoli hozzáférések előkészítése, felülvizsgálata és használatának ellenőrzése az informatikai biztonsági vezető hatáskörébe tartozik a hatályos szabályozás szerint.

Az Ibtv. 11. § (1) bekezdés c) pontja szerint a szervezet vezetője köteles gondoskodni az elektronikus információs rendszer biztonságáért felelős személy kinevezéséről vagy megbízásáról. A felelős személyről tájékoztatást köteles nyújtani a hatóság (Nemzeti Elektronikus Információbiztonsági Hatóság – NEIH) részére, a szervezet a bejelentést elektronikus űrlap (NEIH REG) formájában teheti

meg. Tekintettel arra, hogy egy-egy kisebb önkormányzat esetében nem kivitelezhető egy főállású elektronikus információs rendszer biztonságáért felelős személy alkalmazása, ezért Ludányhalászi Község Önkormányzata úgy döntött, hogy a Szécsény Járási Önkormányzatok Területfejlesztési és Feladatellátási Társulásán keresztül látja el a feladatot. Ennek megfelelően került kinevezésre a kellő szakértelemmel rendelkező felelős személy, akit a NEIH felé is regisztrált az önkormányzat. Elektronikus információs rendszer biztonságáért felelős személy jelenleg is ellátja a feladatait a Társuláson keresztül.

Összességében megállapítható, hogy az önkormányzat rendelkezik szabállyal és felelős személy is kinevezésre került. A szabályozás és a szakember a jogszabályi előírásoknak és követelményeknek megfelel.

1.3 Iratkezelési szabályzat

A Ludányhalászi Község Önkormányzati Hivatal Iratkezelési Szabályzatát 2019 évben hagyta jóvá a Nógrád Megyei Levéltár és a Nógrád Megyei Kormányhivatal. Az új szabályzat az ASP rendszerhez való csatlakozást követően került kiadásra, amely a közokiratokról, közlevéltárakról és a magánlevéltári anyag védelméről szóló 1995. évi LXVI. törvényhez, valamint a közfeladatot ellátó szervek iratkezelésének általános követelményeiről szóló 335/2005. (XII.29.) Korm.rendeletre igazodik. A szabályzatban az egységes irattári terv az önkormányzati hivatalok egységes irattári tervének kiadásáról szóló 78/2012. (XII.29.) Korm. rendelet alapján készült.

Az önkormányzati hatósági ügyekben, illetve egy általános ügyintézés során az önkormányzat természetes és jogi személy ügyfelei részére az Önkormányzati Hivatali Portálon, az ügyfél- és cégkapukon keresztül, illetve az e-Papír szolgáltatás segítségével lehetőséget biztosít az elektronikus ügyintézésre, de az iratok túlnyomórészt még papíralapúak az önkormányzatnál. Az önkormányzat így adatkezelő, hiszen személyes és cégszemélyes adatokat is kezel, vagyis az adatkezelés során keletkezett iratokat a közfeladatot ellátó szervek iratkezelésére vonatkozó jogszabályi követelmények szerint iktatja, és az iktatott iratok között az irat selejtezéséig, illetve annak hiányában levéltárba adásáig kezeli.

Az adatkezelés jogalapja a legtöbb esetben adatkezelő (az önkormányzat) jogi kötelezettségeinek teljesítése. Jogszabályi felhatalmazás alapján más szervek (pl.: bíróság, nyomozó hatóság, közigazgatási hatóság, adóhatóság, bérszámfejtő) tájékoztatás adása, adatok közzétevése, iratok rendelkezésre bocsátása végett megkereshetik az adatkezelőt, az önkormányzatot. Ha más hatóság megjelöli a pontos célt és az átadandó adatokat, akkor az önkormányzat annyi és olyan mértékben adhat ki adatot, amely a megkeresés céljának megvalósításához elegendő, és amire a jogszabályi felhatalmazás alapul ad.

Ha az önkormányzat hozzájáruláson alapuló adatkezelést kíván végezni, az érintett(ek) hozzájárulást a személyes adatai(k) kezeléséhez az adatkérő lap szerinti tartalommal és tájékoztatás mellett kell kérni. Ezért is szükséges az Iratkezelési szabályzat mellett az Adatvédelmi szabályzat és az adatkezelési tájékoztató megléte és ismertetése az ügyfelekkel és a hivatali ügyintézőkkel.

Az Iratkezelési szabályzat megfelel a hatályos jogszabályi előírásoknak, összhangban van az ASP iratkezelési szakrendszerével, az ügyintézők a tartalmát ismerik. Fontos, hogy az önkormányzat az Adatvédelmi és biztonsági szabályzat kidolgozása során az Iratkezelési szabályzatban előírtakat is szem előtt tartsa, valamint a munkaköri leírásokban is rögzítse a kapcsolódó feladatokat.

1.4 Kamerarendszer szabályzat

Ludányhalászi Község Önkormányzatának közigazgatási területén nem kerültek kihelyezésre kamerák. Az önkormányzat épületében, az ügyféltérben nem kerültek kihelyezésre kamerák. Mivel az önkormányzat tulajdonában nincsenek kamerák, kamerarendszert nem működtet, így nincs szükség kamerarendszer működtetésére vonatkozó szabályzatra.

2.Önkormányzati ügyintézés során kezelt adatok

2.1 Ügyféladatok, szerződő partnerek, kapcsolattartók adatainak kezelése

Az önkormányzat szerződés teljesítése jogcímén a szerződés megkötése, teljesítése, megszűnése, szerződési kedvezmény nyújtása céljából kezeli a vele vevőként, szállítóként szerződött természetes személy nevét, születési nevét, születési idejét, anyja nevét, lakcímét, adóazonosító jelét, adószámát.

A vállalkozói, őstermelői igazolvány számát, személyi igazolvány számát, lakcímét, székhely és telephely címét, telefonszámát, e-mail címét, honlap címét, bankszámlaszámát, vevőszámát (ügyfélszámát) és egyéb online azonosítóját. Ezen adatkezelést jogszerűnek minősül akkor is, ha az adatkezelés a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükségesek. A személyes adatok címzettjei az adatokat a szerződés megszűnést követő 5 évig tárolhatják.

Az adatkezelés jogszerűnek minősül, ha arra valamely szerződés vagy szerződéskötési szándék keretében van szükség (Rendelet Preambulum 44.) ha az a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges (Rendeltet 6 cikk (1) b./). A szerződés teljesítése jogcímén a fentiekben leírtak szerint kezelhetők a szerződési ajánlatok keretében gyűjtött személyes adatok is. Ajánlattételkor, illetve fogadáskor erről az önkormányzat köteles az ajánlattevőt, az ajánlat címzettjét tájékoztatni.

Mivel jelenleg nincs hatályban Adatvédelmi szabályzat, a tájékoztatás kizárólag szóban történhet meg.

Az Adatvédelmi Szabályzat elkészítését követően szükséges az írásbeli, illetve az elektronikus módon (honlap) történő tájékoztatás.

2.2. Szociális, gyermekvédelmi ellátások folyósítása céljából kezelt adatok köre

Az önkormányzat jogi kötelezettség teljesítése jogcímén, törvényben ill. helyi önkormányzati rendeletben előírt szociális és gyermekvédelmi ellátások (Szoc.tv., Gyvt., helyi rendelet) céljából kezeli azon érintettek – a támogatásban, ellátásban, juttatásban részesülők – jogszabályban előírt személyes adatait, akikkel kapcsolatban áll. A kezelt adatok körét a Szoc.tv. 18. §-a határozza meg, külön is kiemelve ebből a következőket:

- természetes személy adatai,
- neme,
- állampolgársága,
- természetes személy adóazonosító jele,
- társadalombiztosítási azonosító jele,
- személyi, családi és vagyoni viszonyai (amelyek a kérelem elbírálásához szükségesek).

Az érintett személyek (ügyfelek) jogai a következők:

- átlátható tájékoztatás, kommunikáció az érintett joggyakorlás elősegítése,
- az előzetes tájékozódáshoz való jog (ha a személyes adatokat az érintettől gyűjtik),

- az érintett tájékoztatása és a rendelkezésre bocsátandó információk, ha a személyes adatokat az adatkezelő nem tőle szerezte meg,
- az érintett hozzáférési joga,
- a helyesbítéshez való jog
- a törléshez való jog,
- az adatkezelés korlátozásához való jog,
- a személyes adatok helyesbítéséhez vagy törléséhez, ill. az adatkezelés korlátozásához kapcsolódó értesítési kötelezettség,
- az adathordozhatósághoz való jog
- a tiltakozáshoz való jog,
- automatizált döntéshozatal egyedi ügyekben,
- korlátozások,
- az érintett tájékoztatása az adatvédelmi incidensről,
- felügyeleti hatóságnál történő panasztételhez való jog
- felügyeleti hatósággal szembeni hatékony bírósági jogorvoslathoz való jog
- az adatkezelővel vagy az adatfeldolgozóval szembeni hatékony bírósági jogorvoslathoz való jog.

2.3. Kifizetői adatkezelés (munkaügyi iratok)

Az önkormányzat és intézményei jogi kötelezettség teljesítése jogcímén, törvényben előírt adó- és járulékkötelezettségek (adó-, adóelőleg, járulékok megállapítása, bérszámfejtés, társadalombiztosítási és nyugdíj ügyintézés) céljából kezeli az érintettek (munkavállalók, családtagjaik) adótörvényben előírt személyes adatait, akikkel kifizetői (Art. 7.§ 31. pont) kapcsolatban állnak. A kezelt adatok körét az Art. 50. §-a határozza meg, külön is kiemelve ebből:

- természetes személy személyazonosító adatai,
 - neme,
 - adóazonosító jele,
 - társadalombiztosítási azonosító jele.

Amennyiben az adótörvények egyéb adatokhoz valamilyen jogkövetkezményt fűznek, az önkormányzat kezelheti a munkavállalók egészségügyi (Szja tv. 40. §) és szakszervezeti (Szja tv. 47. § (2) b) tagságra vonatkozó adatokat adó- és járulékkötelezettségek teljesítése céljából.

Közalkalmazottak és köztisztviselők esetében jogszabály előírja, hogy melyek azok az adatok, amelyeket a foglalkoztató nyilvántartási célból kezel. A Kjt. VIII. Fejezete tartalmazza a közalkalmazotti alapnyilvántartás vezetését és a tartalmára vonatkozó előírásokat, míg a Kttv. 2. melléklete pontosan leírja a közszolgálati alapnyilvántartás adatkörét.

2.4. Helyi adóztatás céljából kezelt adatok köre

Az önkormányzat jogi kötelezettség teljesítése jogcímén, törvényben, helyi rendeletben előírt adókimutatás, adóztatás (adókimutatás, adó megállapítás, adóbevallások kezelése, feldolgozása, adóügyi ügyintézés) céljából kezeli azon érintettek – adófizetésre kötelezettek – adótörvényekben előírt személyes adatait, akikkel adóztatási (Art. 7. § 31.) kapcsolatban áll. A kezelt adatok körét az Art. 50. §-a határozza meg, külön is kiemelve: természetes személyek személyazonosító adatai (születési név, születési hely és idő, anyja neve, titulus), nemét, állampolgárságát, adóazonosító jelét, TAJ számát.

2.5. Adó- és számviteli kötelezettségek teljesítése céljából végzett adatkezelés

Az adatkezelő önkormányzat kötelezettség teljesítése jogcímén, törvényben előírt adó- és számviteli kötelezettségek (könyvelés, adózás) teljesítése céljából kezeli a vevőket, szállítóként vele üzleti kapcsolatba lépő természetes személyek törvényben meghatározott adatait. A kezelt adatok az ÁFA tv. 169. § és 202.§ alapján: név, cím, gazdasági műveletet elrendelő személy vagy szervezet megjelölése, az utalványozó és a rendelkezés végrehajtását igazoló személy, valamint a szervezettől függően az ellenőr aláírása; készletmozgások bizonylatain és a pénzügyi bizonylatokon az átvevő, az ellennyugtákon a befizető aláírása, az SZJA törvény alapján a vállalkozói igazolvány vagy őstermelői igazolvány száma, adóazonosító jele. Útnyilvántartás és menetlevél vezetése esetén az adatkezelő jogi kötelezettség jogcímén, költségelszámolás, bizonylatolás, adóalapok megállapítása, üzemanyag megtakarítás elszámolása céljából kezeli a céges és a foglalkoztatott hivatali, üzleti célra használt saját gépjárműhasználatának törvényben meghatározott adatait (gépkocsivezető neve, gépjármű típusa, rendszáma, utazás időpontja és célja, megtett útvonal. A vonatkozó jogszabályok az SZJA tv. 27. § (2) és a 3. melléklet 6. valamint 5. melléklet 7 pont.

3. Adminisztratív védelmi intézkedések (logikai és fizikai)

Az önkormányzat feladata a személyes adatokhoz, személyes adatokat tartalmazó dokumentumokhoz, az elektronikus információs rendszerhez hozzáféréssel rendelkező személyek folyamatos oktatásának, képzésének az elősegítése, az ajánlott elektronikus információbiztonsági eljárások, technikák és technológiák naprakészen tartása. Célként kell megfogalmazni, hogy az önkormányzati tisztviselők tudatában legyenek az adatvédelmi és információbiztonsági elvárásoknak és fenyegetettségeknek, illetve felelősségeiknek. A biztonság tudatosítása a felhasználók esetében oktatások és képzések útján valósulhat meg.

Fontos megismertetni és betartatni a munkavállalókkal, illetve egyéb partnerekkel (pl.: üzemeltetési partnerek) a személybiztonsági előírásokat és szabályokat, az internethasználattal és elektronikus levelezéssel, az elektronikus információs rendszerekkel (pl.: ASP, SZL, ASZA) felhasználó személyekkel szembeni elvárásokat, szabályokat és felelősséget, illetve az adott rendszer használatához kapcsolódó kötelezettségeket és tiltott tevékenységeket. Az adatkezelés, adatfeldolgozás során gondoskodni kell arról, hogy a tárolt adatokhoz belső rendszeren keresztül vagy közvetlen hozzáférés útján kizárólag az arra feljogosított személyek, kizárólag az adatkezeléshez szükséges szinten és célhoz kötötten férjenek hozzá. Az adatkezelők (önkormányzati alkalmazottak, felhasználók) esetében tudatosítani kell, hogy a tőlük elvárható legnagyobb gondossággal járjanak el az adatkezelés során. Meg kell akadályozni a kapott hozzáférési jogokkal való visszaélést, meg kell őrizni a hozzáférési adatok titkosságát. Fontos szem előtt tartani, hogy a felhasználók elszámoltathatók minden olyan tevékenységért, amelyet a saját felhasználói azonosítójával végzett vagy azzal végeztek el. A szerepkörök és jogosultságok változását folyamatosan kezelni szükséges, azok átvezetéséről gondoskodni szükséges (jogok, kötelezettségek, feladatkörök). Jogviszony megszűnésekor pedig az alkalmazottak információhoz és információ-feldolgozó eszközökhöz való hozzáférési jogosultságát meg kell szüntetni, tőlük vissza kell venni a részükre esetlegesen átadott egyéni hitelesítésre szolgáló eszközöket (pl.: kártyaolvasó).

Az adatok feldolgozása, felhasználása során az adathordozók esetében az alábbi biztonsági szabályok betartását javaslom, amelyek az Informatikai biztonsági szabályzatban is megtalálhatóak:

- tilos a munkavégzéshez biztosított információtechnológia vagy számítástechnikai eszköz, rendszer, elektronikus levelezési rendszer használata, az internet hálózat feladatellátáson kívüli használata,

- a hivatalos levelezőrendszer csak szervezeti célokra alkalmazható, ha a tisztviselők nem a munkavégzéshez kapcsolódó elektronikus levelet, vagy csak egy csatolmányt kapnak, azokat haladéktalanul töröljék
- javasolt a tisztviselők részére egyéni, teljes névvel ellátott, az önkormányzat által használt domain nevű egyedi e-mail címek létrehozása és használata a jelenlegi ingyenes levelezők helyett,
- tilos más postafiókjához felhatalmazás nélkül hozzáférni,
- tilos az elektronikus információs rendszerek biztonsági beállításainak megváltoztatása, illetve a vírusellenőrzők kikapcsolása és módosítása,
- a munkáltató korlátozhatja a felhasználók esetében egyes internetes oldalakhoz való hozzáférést, a felkeresett internetes oldalakat a munkáltató naplózhatja.

Össességében megállapítható, hogy az önkormányzat az adatvédelmi szempontok betartását szem előtt tartja, logikai védelmi eszközöket (jelszavakat) használ az adatkezelés során a legtöbb információs rendszer használata során. A számítógépek logikai védelme érdekében a felhasználókhöz szükséges jelszavakat rendelni, a jelszavakat pedig titkosan kezelni, esetleges helyettesítések esetében pedig a megfelelő szintű hozzáféréseket szükséges biztosítani.

Ludányhalászi, 2021. április 21.


 Csépe Péter
 Belső ellenőr

Megismerési záradék.

Alulírott kijelentem, hogy az ellenőrzési jelentésben foglaltakat megismertem. A javaslatok érvényesülésére a költségvetési szervek belső kontrollrendszeréről és belső ellenőrzéséről szóló 370/2011.(XII.31) Kormány rendelet 45 §. 1-3 bekezdése értelmében a jelentés kézhezvételétől számított **8 napon belül** intézkedési tervet készítek és a szükséges intézkedéseket megteszem.

A költségvetési szervek belső kontrollrendszeréről és belső ellenőrzéséről szóló 370/2011.(XII.31) Kormány rendelet 42 §. 2 bekezdése értelmében az ellenőrzési jelentéssel kapcsolatosan

- észrevételt nem teszek*
- 8 napon belül észrevételt kívánok tenni*

*(A megfelelő rész aláhúzendó)

Ludányhalászi, 2021. április 21.


Németh Ilona
Jegyző



Kapják: Szécsény Járási Önkormányzatok Területfejlesztési és Feladatellátási Társulás
Ludányhalászi Község Önkormányzat
Belső ellenőr