ADATVÉDELMI ÉS ADATBIZTONSÁGI SZABÁLYZAT

I. fejezet

ÁLTALÁNOS RENDELKEZÉSEK

1. § (1) Az Adatvédelmi és Adatbiztonsági Szabályzat (a továbbiakban: Szabályzat) célja, hogy meghatározza a szervezeti hatályban rögzített szerveknél folytatott személyes adatok kezelésének jogszerű rendjét, valamint biztosítsa az adatvédelem alkotmányos elveinek, az információs önrendelkezési jognak és az adatbiztonság követelményeinek érvényesülését.

(2) A Szabályzatot az általános adatvédelmi rendelet (a továbbiakban: „általános adatvédelmi rendelet", vagy „GDPR"), valamint az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) 2. § (2) bekezdése szerint azt kiegészítő előírásokra figyelemmel, továbbá az alkalmazandó ágazati jogszabályi követelményekkel összhangban kell alkalmazni.

(3) A szervekhez beérkező és a náluk keletkezett iratok készítésének, kezelésének, nyilvántartásának, irattározásának és selejtezésének alapvető szabályait, az iratkezeléssel összefüggő adatvédelmi és adatbiztonsági szabályokat az Iratkezelési Szabályzattal összhangban kell alkalmazni.

(4) Az elektronikus információs rendszerekben tárolt személyes adatok védelmére irányuló követelményeket az Informatikai Biztonság Szabályzatban meghatározottakkal összhangban kell alkalmazni.

(5) A Szabályzatban alkalmazott fogalmak tekintetében az általános adatvédelmi rendelet 4. cikke szerinti meghatározások az irányadók.

II. fejezet

A SZABÁLYZAT HATÁLYA

2. § (1) Jelen Szabályzat kötelezően alkalmazandó az alábbi szervekre és intézményekre:

- Apostag Község Önkormányzata
  Székhely: 6088 Apostag, Kossuth Lajos utca 1.
  A Szabályzat végrehajtásáért felelős: Polgármester
  Hatálybalépés: 2026. március 1.

- Dunaegyháza Község Önkormányzata
  Székhely: 6323 Dunaegyháza, Mikszáth Kálmán u. 25.
  A Szabályzat végrehajtásáért felelős: Polgármester
  Hatálybalépés: 2026. március 1.

- Apostagi Közös Önkormányzati Hivatal
  Székhely: 6088, Apostag, Kossuth L. u. 1.
  A Szabályzat végrehajtásáért felelős: Jegyző
  Hatálybalépés: 2026. március 1.

- Pöttömkert Óvoda
  Székhely: 6088 Apostag, Hunyadi utca 25.
  A Szabályzat végrehajtásáért felelős: Igazgató
  Hatálybalépés: 2026. március 1.

-Dunaegyházi Mákszem Óvoda
  Székhely: 6323 Dunaegyháza, Mikszáth K. u. 36.
  A Szabályzat végrehajtásáért felelős: Igazgató
  Hatálybalépés: 2026. március 1.

(2) Az (1) bekezdésben felsoroltak a személyes adatok kezelése során önálló adatkezelőnek minősülnek.

Az Apostagi Közös Önkormányzati Hivatal a jogszabályban, valamint a felek között létrejött munkamegosztási megállapodásokban meghatározott feladatok ellátása során – az adatkezelés céljának és lényeges körülményeinek meghatározása nélkül – adatfeldolgozóként jár el (pl. bérszámfejtés, ASP-rendszer üzemeltetés, iktatás). Azon adatkezelések tekintetében, amelyek esetében a Közös Önkormányzati Hivatal a jogszabály alapján önálló döntési jogkörrel rendelkezik, önálló adatkezelőnek minősül.

3. § Jelen Szabályzat 2026. március 1. napján lép hatályba és visszavonásig érvényes.

4. § A Szabályzat személyi hatálya kiterjed az Önkormányzatok Polgármestereire, Képviselő-testületeire, a foglalkoztatottakra, a Közös Hivatal, az Óvodák vezetőire és alkalmazottaira, valamint mindazon személyekre, akik a szervezetekkel jogviszonyban állva személyes adatokat kezelnek.

5. § A Szabályzat tárgyi hatálya kiterjed valamennyi kezelt személyes adatra, az adatkezelés során alkalmazott informatikai és papíralapú nyilvántartásokra, valamint az adatkezelést szolgáló hardver- és szoftvereszközökre.

III. fejezet

AZ ADATVÉDELMI RENDSZER

A személyes adatokkal kapcsolatos felelősségek

6. § (1) A személyes adatok védelméért, az adatkezelés jogszerűségéért az Önkormányzatok felelősek. Ennek keretében

a) kötelező utasítások útján meghatározzák a személyes adatok védelme és az adatkezelés jogszerűsége szempontjából elvárt, megfelelő technikai és szervezési intézkedéseket és rendelkezik azok folyamatos alkalmazásáról és naprakészen tartásáról;

b) gondoskodnak az adatkezelés személyi és tárgyi feltételeinek biztosításáról, az adatvédelmi és adatbiztonsági rendszer működtetéséről, a működéshez szükséges intézkedések megtételéről;

c) kijelölik az adatvédelmi tisztviselőt;

d) meghozzák a szerv, mint adatkezelő tekintetében az adatkezelésre vonatkozó döntéseket;

e) felelnek az önkormányzati honlapokon az adatkezelési tevékenységével kapcsolatos közzétételi kötelezettség teljesítéséért.

(2) Az Önkormányzatok az adatkezelés személyi és tárgyi feltételeinek biztosításáról, a Szabályzatban foglaltak végrehajtásáról, az adatvédelemmel kapcsolatos szabályok foglalkoztatottak általi megismeréséről és betartásáról a szervek vezetői által gondoskodnak.

(3) Az Önkormányzatok az adatkezeléssel kapcsolatos döntések előkészítését, az elszámoltathatóság érdekében szükséges dokumentáció és intézkedések tervezetének összeállítását a Szervezeti és Működési Szabályzatokban meghatározottak szerint a Közös Önkormányzati Hivatal útján végzik.

7. § Az önálló szervezeti egységek vezetői gondoskodnak a szervezeti egységük állományába tartozó foglalkoztatott személyek kapcsán

a) az adatvédelmi követelmények érvényre juttatásáról;

b) a Szabályzatban vagy más kötelező erejű adatvédelmi előírásban foglaltak ellenőrzéséről, azok megsértése esetén a hiányosságok haladéktalan felszámolásáról;

c) a szükséges hozzáférési jogosultságok kiadására és visszavonására irányuló előterjesztésekről;

d) az adatvédelmi tudatosító – ideértve az adatvédelmi incidenskezeléssel, a kapcsolódó információbiztonsággal, valamint az iratkezeléssel összefüggő ismereteket is – képzéseken történő részvételről, szükség esetén ilyen képzés szervezésének kezdeményezéséről.

8. § (1) A foglalkoztatottak

a) a Szabályzatban meghatározottak szerint kezelik a feladataik ellátásával összefüggésben tudomásukra jutott személyes adatokat;

b) betartják az adatkezelésre vonatkozó jogszabályokban, más belső szabályzatokban foglalt előírásokat;

c) tudásukat naprakészen tartják a munkavégzésükre irányadó adatvédelmi és adatbiztonsági előírások kapcsán és az adatvédelmi incidensek gyanújának felismerése érdekében.

(2) Az adatvédelmi előírások és jelen Szabályzat előírásainak megszegője a közszolgálati tisztviselőkről szóló 2011. évi CXCIX. törvény, a közalkalmazottak jogállásáról szóló 1992. évi XXXIII. törvény, a Munka törvénykönyvéről szóló 2012. évi I. törvény, vagy a pedagógusok életpályájáról szóló 2023. évi LII. törvény szerinti fegyelmi felelősséggel tartozik.

(3) Ha a személyes adatok védelmével kapcsolatos előírások megsértése miatt jogerősen sérelemdíj, kártérítés, hatósági bírság fizetési kötelezettség keletkezik, a jogsértést elkövető foglalkoztatottat, foglalkoztatottakat a közszolgálati tisztviselőkről szóló 2011. évi CXCIX. törvény, a közalkalmazottak jogállásáról szóló 1992. évi XXXIII. törvény, a Munka törvénykönyvéről szóló 2012. évi I. törvény, vagy a pedagógusok életpályájáról szóló 2023. évi LII. törvény szerinti kártérítési felelősség terheli.

9. § Az adatvédelmi tisztviselő közvetlenül az Önkormányzatok Polgármestereinek felel, függetlenül és befolyásolástól mentesen látja el az általános adatvédelmi rendeletben és az e Szabályzatban meghatározott feladatait.

A szervezeten kívüli személyek bevonása az adatkezelés folyamatába

10. § (1) Amennyiben a szervek vezetőinek döntése alapján a közfeladat ellátása érdekében adatfeldolgozó igénybevétele szükséges, úgy az általános adatvédelmi rendelet 28. cikke szerinti tartalommal az adatfeldolgozó felelősségét önálló szerződésben vagy a felek között létrejövő szolgáltatási szerződés részeként kell rögzíteni. A szerződés tartalmának összeállítása során ki kell kérni az adatvédelmi tisztviselő véleményét.

(2) A (1) bekezdésben foglalt kötelezettség nem alkalmazandó annyiban, amennyiben az adatfeldolgozó igénybevételének kereteit és garanciális feltételeit jogszabály határozza meg.

11. § A szerződéses jogviszonyba kerülő önálló adatkezelő mint címzett kapcsán a szerződés részeként szükséges rendelkezni a személyes adatok védelme és biztonsága érdekében

alkalmazandó intézkedésekről. A szerződés adatkezelést érintő részének összeállítása során ki kell kérni az adatvédelmi tisztviselő véleményét.

Az adatvédelmi tisztviselő kinevezése, jogállása és feladatai

12. § (1) Az Önkormányzatok a Közös Önkormányzati Hivatal által kötött szerződés útján határozatlan időre, írásos szerződésben bízzák meg az adatvédelmi tisztviselőt.

(2) Adatvédelmi tisztviselői feladatot nem láthat el olyan személy, aki az Önkormányzatoknál adatkezeléssel kapcsolatos érdemi döntések meghozatalára jogosult személy a Polgári Törvénykönyvről szóló 2013. évi V. törvény 8:1. § (1) bekezdés 2. pontja szerinti hozzátartozója.

(3) Az adatvédelmi tisztviselő számára biztosítani kell, hogy – a GDPR-ban és más jogszabályban, valamint az e Szabályzatban meghatározott feladatainak ellátása céljából és az ahhoz szükséges mértékben – minősített adatot is megismerjen, minősítéssel jelölt iratokba betekinthessen.

(4) Az adatvédelmi tisztviselő nevét és elérhetőségét az Önkormányzatok honlapján közzétett adatkezelési tájékoztatók útján nyilvánosan elérhetővé kell tenni, kijelöléséről az Önkormányzatok intézményeit tájékoztatni kell.

13. § (1) Az Önkormányzatok biztosítják az adatvédelmi tisztviselő számára a hozzáférést és a megfelelő jogosultságokat a feladatai végrehajtásához szükséges elektronikus rendszerekhez, iratokhoz, egyéb adatokhoz, valamint a rendelkezésére bocsátják a feladatai ellátásához és szakmai ismeretei naprakészen tartásához szükséges eszközöket és erőforrásokat.

(2) A Közös Önkormányzati Hivatal segíti az adatvédelmi tisztviselőt a Szabályzat szerinti feladataik ellátása kapcsán, valamint felel a Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: NAIH) online adatvédelmi tisztviselő bejelentő rendszerében és az adatkezelési tájékoztatókban az adatvédelmi tisztviselő nevének és elérhetőségének naprakészen tartásáért.

(3) Az adatvédelmi tisztviselő tisztségével összefüggő kötelezettségei és feladatai ellátása során nem utasítható, és e tisztségének ellátásával kapcsolatban közvetlenül az Önkormányzatoknak tartozik beszámolási kötelezettséggel.

(4) Amennyiben az adatvédelmi tisztviselő összeférhetetlenséget állapít meg valamely általa ellátandó feladattal összefüggésben, úgy erről köteles haladéktalanul értesíteni a Polgármestereket, akik a feladat kapcsán eseti adatvédelmi tisztviselőt alkalmaznak.

14. § Az adatvédelmi tisztviselő a GDPR 39. cikkében foglalt feladatai mellett

a) vezeti a Szervek adatvédelmi nyilvántartását;

b) adatvédelmi ellenőrzéseket végezhet, melyek eredményéről a Polgármestereket tájékoztatja;

c) az adatvédelmi ellenőrzés során – szükség szerint azon túl is, különösen érintettől érkező, az adatkezelést érintő panasz, vagy adatvédelmi incidens bekövetkezte esetén – ellenőrzi az adatvédelmi és adatbiztonsági követelmények teljesülését;

d) közreműködik az adatvédelmi incidens kezelésében, kivizsgálásában, és a vizsgálat eredménye alapján az adatvédelmi incidenst a GDPR 33. cikke szerint bejelenti a NAIH részére;

e) a személyes adatok kezelését igénylő új tevékenység ellátásáért felelős szervezeti egység kérésére előzetesen is véleményezi a tervezett adatkezelést;

f) megvizsgálja a tervezett vagy módosuló adatkezelések érintettekre gyakorolt kockázatát, szükség esetén adatvédelmi hatásvizsgálatot kezdeményez és közreműködik annak lefolytatásában;

g) adatvédelmi szempontból véleményezi az adatfeldolgozóval, közös adatkezelővel vagy más önálló adatkezelővel kötendő megállapodást;

h) új adatkezeléssel járó tevékenység tervezése vagy valamely adatkezelés körülményeinek változása esetén megvizsgálja, hogy szükséges-e azzal kapcsolatban adatkezelési tájékoztató, új adatvédelmi nyilvántartás bejegyzés, vagy más dokumentáció összeállítása, illetőleg a már létező dokumentum módosítása;

i) kezdeményezi a munkatársak adatvédelmi tudatosító képzését, részt vesz az ilyen képzéssel kapcsolatos feladatok ellátásában, képzést tart;

j) elősegíti az érintetteket megillető jogok gyakorlását, valamint véleményezi a beérkező, érintetti joggyakorlásra irányuló beadványokra összeállított válaszok tervezetét;

15. § (1) A Szabályzat hatálya alá tartozó adatkezelés érintettje a személyes adatai kezeléséhez és jogai gyakorlásához kapcsolódó bármely kérdésben – a hivatali út betartása nélkül, közvetlenül és szabadon megválasztott kapcsolattartási mód szerint – az adatvédelmi tisztviselőhöz fordulhat.

(2) Saját helyzetéből fakadó okokra hivatkozva bármely érintett jogosult kérni, hogy az adatvédelmi tisztviselő ne fedje fel kilétét a szerv vezetője, vagy bármely más foglalkoztatottja előtt. Az adatvédelmi tisztviselő a kérésnek köteles eleget tenni, még akkor is, ha ennek hiányában a panaszolt adatvédelmi probléma nem orvosolható, azonban erről köteles tájékoztatni az érintettet.

(3) Az (1) bekezdés szerinti panaszt, ha az annak kivizsgálásához szükséges minden releváns információ rendelkezésre áll, az adatvédelmi tisztviselő köteles a GDPR szerinti határidő figyelembe vételével kivizsgálni, és a vizsgálat eredményéről értesíteni az érintettet.

16.§ (1) Az adatvédelmi tisztviselő jogosult

a) tájékoztatást, felvilágosítást kérni minden, e Szabályzat hatálya alá tartozó adatkezelésről;

b) minden, e Szabályzat hatálya alá tartozó adatkezelést vizsgálni és minden olyan helyiségbe belépni, ahol adatkezelés folyik;

c) tanácskozási és véleményezési joggal részt venni minden olyan Képviselő-testületi ülésen, ahol a feladatai ellátásával összefüggő kérdések szerepelnek a napirenden,

d) javaslatot tenni közvetlenül a Képviselő-testületeknek valamely személyes adatok kezelését érintő kérdésben.

(2) Az adatvédelmi tisztviselő az ellenőrzései kapcsán és a vizsgálataival összefüggésben a fentiek mellett

a) felszólíthatja az adatkezelésben résztvevő személyt a jogszerű állapot helyreállítására;

b) kisebb súlyú ügyben közvetlenül az adatkezelésért felelős önálló szervezeti egység vezetőjénél kezdeményezheti az alkalmazott adatkezelési gyakorlat felülvizsgálatát;

c) kezdeményezheti az Önkormányzatoknál a vonatkozó adatvédelmi előírások, valamint a kialakult adatkezelési gyakorlat átalakítását, vagy az adatkezelést érintő más szükséges intézkedések megtételét.

IV. Fejezet

A BEÉPÍTETT ÉS ALAPÉRTELMEZETT ADATVÉDELEM ELVÉNEK ÉRVÉNYESÜLÉSE

Adatkezelés kialakításával összefüggő kötelezettségek

17. § (1) A személyes adatok kezelésével járó új tevékenység megkezdése, vagy a folyamatban lévő adatkezelési tevékenységekkel kapcsolatos módosítások hatályba lépése előtt a feladat ellátásáért felelős szervezeti egység vezetője az adatvédelmi tisztviselő véleményének kikérését követően kezdeményezi a Polgármesternél az adatkezelés jogszerű kialakítása, illetve az elszámoltathatóság elvének történő megfelelés érdekében szükséges és arányos intézkedések meghozatalát.

(2) Az (1) bekezdés szerinti megkeresésben az adatkezeléssel járó feladat ellátásáért felelős szervezeti egység vezetője rögzíti a tervezett adatkezelés legfontosabb jellemzőit, így legalább

a) az adatok kezelésére okot adó körülményt, vagy jogszabályi rendelkezést;

b) a feladat ellátásához szükséges adatköröket és azok tervezett forrását;

c) a tervezett vagy jogszabályban meghatározott megőrzési időt, vagy az annak meghatározásához szükséges szempontokat;

d) az ahhoz kapcsolódó adattovábbítás címzettjeit;

e) az adatok biztonsága, valamint az érintettekre nézve azonosított kockázatok csökkentése érdekében tervezett intézkedéseket.

(3) A (2) bekezdés szerinti értesítést a Polgármesterek kötelesek érdemben megvizsgálni; az adatvédelmi tisztviselő véleményét azzal kapcsolatban kikérni; majd az alapján – szükség esetén az előterjesztő szervezeti egységgel történő konzultáció, az értesítés kiegészítése vagy pontosítására történő felhívást követően – javaslatot tenni a Képviselő-testületnek

a) az ahhoz kapcsolódóan szükségesnek tartott további szervezési és technikai intézkedésekre, vagy a GDPR 5. cikkében foglalt alapelveknek megfelelő adatkezelés kialakításának szempontjaira nézve;

b) a kapcsolódó adatvédelmi hatásvizsgálat szükségessége kapcsán;

c) az ahhoz kapcsolódó adatkezelési tájékoztató tartalmára és esetleges közzétételére vonatkozóan.

(4) Ha a tervezett adatkezelés kapcsán alkalmazandó a meghatározott rendszeres felülvizsgálati kötelezettség, a javaslat a rendszeres felülvizsgálat lefolytatásának időpontjára és módjára is ki kell, hogy térjen.

(5) A (3) bekezdés szerinti javaslat kapcsán hozott döntésről a Polgármester tájékoztatja a személyes adatkezeléssel járó feladat ellátásáért felelős önálló szervezeti egység vezetőjét, valamint a tevékenység adatvédelmi nyilvántartásba történő bejegyzése érdekében az adatvédelmi tisztviselőt.

18. § (1) Kizárólag akkor hivatkozható a szervek adatkezelési tevékenysége kapcsán a GDPR 6. cikk (1) bekezdés e) pontja szerinti jogalap helyett más, a GDPR 6. cikkében foglalt jogalap, ha az adatkezelési tevékenység nem szükséges a közfeladat ellátásához, vagy közhatalmi tevékenység gyakorlásához.

(2) Az (1) bekezdésben foglaltakon túl is kizárólag akkor képezheti a adatkezelés jogalapját a GDPR 6. cikk (1) bekezdés a) pontja szerinti érintetti hozzájárulás, ha az adatkezelés vonatkozásában igazolható módon nincs az érintett és a szerv között egyértelműen egyenlőtlen viszony, továbbá szervezési és technikai intézkedésekkel biztosítható, hogy az érintett hozzájárulását bármikor ugyanolyan könnyen visszavonhassa, ahogy azt megadta.

19. § (1) Személyes adatokat továbbítani kizárólag pontosan meghatározott és jogszerű célból, a konkrét esetben közvetlenül hivatkozható jogalap birtokában lehetséges, és a továbbítandó adatok körét az alkalmazandó jogszabályi követelményeket és az iratkezelésre vonatkozó belső előírásokat is mérlegelve az adatkezelés céljához szükséges körre kell szűkíteni.

(2) Amennyiben a kezelt személyes adatok továbbítására nem az önkormányzati ASP rendszerben iktatott módon kerül sor, úgy arról az adattovábbítással járó feladat ellátásáért felelős önálló szervezeti egység elektronikus úton nyilvántartást köteles vezetni.

Adatbiztonsági követelmények

20. § (1) A szervek kezelésében lévő személyes adatok bizalmasságát, sértetlenségét és rendelkezésre állását biztosítandó, az érintettekre nézve megjelenő kockázatokkal arányos, a technológiai fejlődés szempontjából naprakész, zárt, teljes körű és folytonos szervezési és technikai védelmi intézkedéseket alkalmaznak.

(2) Az alkalmazott védelmi intézkedések naprakészen tartása érdekében a feladatkörük kapcsán az önálló szervezeti egységek vezetői, valamint az információbiztonsági felelős és az adatvédelmi tisztviselő írásban javaslatot tehet azok pontosítására vagy fejlesztésére a Polgármestereknek.

(3) A szervek elektronikus információs rendszereihez és – a tevékenységével összefüggésben ellátott feladatok ellátásához szükséges – más szerv kezelésében lévő elektronikus információs rendszerekhez, valamint nem elektronikus úton vezetett nyilvántartásokhoz történő hozzáférési jogosultságot és annak szintjét az önálló szervezeti egység vezetője adja meg, illetve vonja vissza, vagy kezdeményezi a rendszer üzemeltetőjénél.

(4) A jogosultságok naprakészségét a hozzáférést kezdeményező önálló szervezeti egység vezetője köteles évente ellenőrizni.

(5) A feladatellátással összefüggő személyes adatokat is tartalmazó iratot vagy adathordozót az önálló szervek épületéből kivinni – munkaköri feladat ellátásának kivételével – csak a szerv vezetőjének engedélyével lehet. A foglalkoztatott ez esetben is köteles gondoskodni az adatbiztonsági követelmények megvalósulásáról.

(6) A közös használatú helyiségeiben és közös használatú eszközök kapcsán – így különösen nyomtatók, másológépek, irattárolók esetében – a személyes adatok célhoz kötött felhasználását, valamint integritását és bizalmas jellegét garantáló további előírásokat jogosult a foglalkoztatottak számára meghatározni az érintett önálló szervezeti egység vezetője.

(7) A szakmai gyakorlatot teljesítő, vagy foglalkoztatásra irányuló jogviszonyban nem álló kutatási tevékenységet végző személy a kezelésben lévő irathoz és elektronikus információs

rendszerhez kizárólag titoktartási nyilatkozat aláírását, továbbá a kezelt adatok biztonságát garantáló szervezési és műszaki intézkedések kialakítását követően férhetnek hozzá.

21. § Az ügyfél és jogos érdekét igazoló harmadik személy az általános közigazgatási rendtartásról szóló 2016. évi CL. törvény (a továbbiakban: Ákr.) hatálya alá tartozó eljárásban iratbetekintési jogának személyes, vagy képviselője útján történő gyakorlása során, valamint az eljárás során keletkezett iratról való másolat, kivonat készítésekor kiemelt figyelmet kell fordítani a bizalmasság elvének történő megfelelés érdekében a törvény által előírt garanciákra és korlátozó rendelkezésekre, így különösen a zárt adatkezeléssel kapcsolatos feladatokra.

Az adatkezelési műveletek átláthatóságára vonatkozó követelmények

22. § (1) A szervezeti egységek adatkezelési tevékenységeire vonatkozóan az adatkezelés érintettje számára világos, könnyen értelmezhető és átlátható módon, az adatkezelés céljai mentén a GDPR 13-14. cikke szerinti tartalommal szükséges az adatkezelési tájékoztatókat összeállítani.

(2) Az adatkezelési tájékoztatókban foglaltak tartalmi megfelelőségét, naprakészségét és elérhetőségét az adatvédelmi tisztviselő és a meghatározott feladataihoz kötődően a tevékenység ellátásáért felelős önálló szervezeti egység is köteles figyelemmel kísérni.

(3) A kizárólag a foglalkoztatottakat érintő adatkezelési célok kapcsán összeállított adatkezelési tájékoztatókat a szervezeti egységekben kell a foglalkoztatottak számára elérhetővé tenni.

(4) A foglalkoztatotti jogviszonyt létesítő személyek számára a belépéshez szükséges dokumentációval együtt, elektronikus úton szükséges megküldeni az őket érintő adatkezelési tájékoztatókat.

(5) A személyesen megjelenő érintetteket, a rájuk vonatkozó adatkezelésekről a szervezeti egységek épületeiben elérhető papíralapú adatkezelési tájékoztató, valamint figyelemfelhívó jelzés útján kell tájékoztatni. Emellett szükség esetén, így különösen látássérültek vagy olvasási, szövegértési képességükben korlátozott érintettek esetében szóbeli tájékoztatás nyújtása is kötelező.

(6) A (3)-(5) bekezdésben nem szabályozott érintetti kör esetében az Önkormányzatok honlapján, az „Adatkezelési tájékoztatók" cím alatt közzétéve bocsátja az érintettek rendelkezésére a szükséges tájékoztatást.

Az adatkezelési tevékenységek nyilvántartása

23. § (1) Az adatvédelmi tisztviselő elektronikusan, az adatkezelők informatikai rendszerében vezeti az adatkezelési tevékenységek nyilvántartását.

(2) Az adatkezelési tevékenységek nyilvántartása az adatkezelési célok mentén, a GDPR 30. cikke által meghatározott tartalommal összeállított nyilvántartás bejegyzésekből áll, amelynek összhangban kell lennie a kapcsolódó adatkezelési tájékoztatókban foglaltakkal.
(3) A nyilvántartás aktualizálását, szükséges módosítását az adatvédelmi tisztviselő végzi.

Az adatvédelmi hatásvizsgálat lefolytatása

24. § (1) Amennyiben egy tervezett adatkezelés kapcsán az adatvédelmi hatásvizsgálat lefolytatásának GDPR 35. cikkében, vagy az Infotv. 25/G. §-ban foglalt feltételei fennállnak – mivel annak jellege, hatóköre, körülményei és céljai, vagy az alkalmazott technológiai megoldások kapcsán az valószínűsíthetően magas kockázattal jár az érintettre nézve, vagy a tervezett adatkezelés a NAIH által a GDPR 35. cikk (4) bekezdése szerint összeállított jegyzékében szerepel – a szerv vezetője kezdeményezi annak lefolytatását.

(2) Az adatvédelmi hatásvizsgálat lefolytatásának GDPR 35. cikkében foglalt feltételei fennállásának vizsgálata keretében figyelemmel kell lenni arra is, hogy alkalmazható-e valamely, a lefolytatás kötelezettsége alóli kivételszabály, így különösen a kötelező adatkezelést előíró jogszabály kapcsán készült-e adatvédelmi hatásvizsgálat, illetve elérhető-e azonos tárgyban készült adatvédelmi hatásvizsgálat.

(3) A kezdeményezésnél figyelembe kell venni

a) az adatvédelmi hatásvizsgálat lefolytatására okot adó legfontosabb szempontokat;

b) az alkalmazni javasolt módszertant;

c) az adatvédelmi hatásvizsgálatot lefolytató munkacsoportba bevonni tervezett szervezeti egységeket és személyeket;

d) a tervezett adatkezelés érintettjei véleményének kikérése kapcsán javasolt megoldást, vagy annak jogszerű mellőzésére okot adó körülményeket;

e) amennyiben az előre megítélhető, a hatásvizsgálat lefolytatásának tervezett időrendjét.

(4) A szervezeti egység vezetője kikéri az adatvédelmi tisztviselő álláspontját az adatvédelmi hatásvizsgálat szükségessége kapcsán, majd elrendeli az adatvédelmi hatásvizsgálat lefolytatását vagy írásban rögzíti mellőzésének okait.

25. § (1) Az adatvédelmi hatásvizsgálatot lefolytató munkacsoportba a tervezett adatkezeléssel érintett önálló szervezeti egységek kötelesek résztvevőt kijelölni.

(2) Az Európai Adatvédelmi Testület által elfogadott – vagy a GDPR alkalmazandóvá válását követően fenntartott –, az adatvédelmi hatásvizsgálatra vonatkozó hatályos iránymutatásban foglalt szempontokat és eljárásrendet a munkacsoport köteles figyelembe venni.

(3) A munkacsoport az adatvédelmi hatásvizsgálat lefolytatását követően megállapításairól és javaslatairól összefoglaló jelentést készít a szervezeti egység vezetőjének. A munkacsoport tevékenysége során keletkezett iratanyag a jelentés kivételével döntés-előkészítő iratnak minősül.

(4) Az adatvédelmi hatásvizsgálatot lefolytató munkacsoport munkáját az adatvédelmi tisztviselő – és amennyiben az adatkezelés elektronikus információs rendszert is érint, az elektronikus információs rendszer biztonságáért felelős személy – segíti. Véleményét legalább a kockázatelemzés, a tervezett intézkedések és az összefoglaló jelentés kapcsán ki kell kérni.

(5) Az adatvédelmi hatásvizsgálatról készült jelentést és a kapcsolódó véleményeket a szervezeti egység vezetője részére kell előterjeszteni.

A tervezett adatkezelés nem kezdhető meg, amíg a szervezeti egység vezetője el nem fogadja

a) az adatvédelmi hatásvizsgálat eredményes lezárultáról, és az abban a kockázatok csökkentését szolgáló intézkedések bevezetéséről és az adatkezelés jóváhagyásáról szóló jelentést, vagy

b) az adatvédelmi hatásvizsgálat mellőzésének, vagy megszüntetésének okait tartalmazó jelentést.

V. Fejezet

AZ ADATVÉDELMI INCIDENSEK KEZELÉSÉVEL KAPCSOLATOS FELADATOK

26. § (1) Amennyiben bármelyik szervezeti egység foglalkoztatottja adatvédelmi incidens bekövetkezésének gyanúját észleli, haladéktalanul tájékoztatja arról az önálló szervezeti egységének vezetőjét. Az önálló szervezeti egység vezetője az általa észlelt adatvédelmi incidens kapcsán saját hatáskörben jár el.

(2) Az önálló szervezeti egység vezetője vagy az általa kijelölt személy az (1) bekezdés szerinti jelzést követően azonnal tájékozódik az eset lényeges körülményeiről.

(3) Amennyiben a rendelkezésre álló adatok alapján egyértelműen megállapítható, hogy az azt észlelő önálló szervezeti egység tevékenységével összefüggésben, vagy azt érintően következett be az adatvédelmi incidens, soron kívül megkezdi az incidens érintettekre nézve megjelenő hatásainak csökkentését és arról haladéktalanul írásban értesíti az adatvédelmi tisztviselőt.

(4) A (3) bekezdés szerinti értesítés az adatvédelmi incidens bekövetkeztének, illetőleg az általa az érintettre nézve jelentett kockázatok és annak hatásainak megállapítása érdekében tartalmazza legalább

a) az adatvédelmi incidens jellegét és rövid leírását, ideértve különösen az észlelés és bekövetkezés feltételezett időpontját, az érintett rendszer vagy irat megjelölését;

b) a valószínűsíthetően érintett személyek körét;

c) a valószínűsíthetően érintett személyes adatok kategóriáit, nagyságrendjét;

d) az általa megtett halaszthatatlan intézkedéseket;

e) megítélése szerint az érintettek jogaira és szabadságaira gyakorolt hatásának súlyosságát,

f) az általa tervezett további intézkedések leírását.

(5) Az önálló szervezeti egység vezetője haladéktalanul értesíti az adatvédelmi tisztviselőt a bekövetkezett eseményről és a nála rendelkezésre álló információról, ha

a) az adatvédelmi incidens bekövetkezte vagy annak (4) bekezdés szerinti jellemzői számára nem állapíthatók meg egyértelműen és legfeljebb az észlelését követő 24 órán belül,

b) az adatvédelmi incidens megítélése szerint elsősorban más önálló szervezeti egység tevékenységét érinti, illetőleg

c) az adatvédelmi incidens több önálló szervezeti egységet is érinthet.

(6) Az adatvédelmi tisztviselő megvizsgálja a (4) vagy (5) bekezdés szerinti értesítésben foglaltakat, és az adatvédelmi incidens lehetséges hatásainak felmérése és megállapítása érdekében szükség szerint bevonja az informatikai biztonságért felelős személyt és informatikusokat, az önálló szervezeti egység vezetőjét vagy az adatvédelmi incidenssel érintett szakterület tekintetében szakértelemmel rendelkező személyeket is.

(7) Abban az esetben, ha az adatvédelmi incidens feltételezhetően az önálló szervezeti egység által üzemeltetett elektronikus információs rendszerek biztonságával összefüggésben következett be, az adatvédelmi tisztviselő az elektronikus információbiztonságért felelős személy felé is köteles jelezni a bejelentést. Az elektronikus információbiztonságért felelős személy a jelzést követően köteles haladéktalanul véleményt összeállítani az adatvédelmi tisztviselő részére arról, hogy az adatvédelmi incidens valóban érinti-e az informatikai rendszer biztonságát, és ismerteti az ezzel kapcsolatos javasolt, valamint megtett intézkedéseket.

(8) Amennyiben az adatvédelmi incidens a szervezeti egység által igénybevett adatfeldolgozó tevékenységével kapcsolatban következett be, az adatvédelmi incidens körülményeinek, és az azzal összefüggő lehetséges kockázatok és hatások(6) bekezdés szerinti kivizsgálásába az adatfeldolgozó képviselőjét is be kell vonni.

(9) Az adatvédelmi tisztviselő a (6) bekezdés szerinti vizsgálata keretében mérlegeli az adatvédelmi incidens következtében az érintettekre nézve megjelenő kockázatokat. Ennek során legalább a következőket veszi figyelembe:

a) az adatvédelmi incidens jellegét;

b) az érintettek körét, hozzávetőleges számukat;

c) az incidenssel érintett adatok kategóriáit, az érintett különleges adatokat és a GDPR preambulumának (75) bekezdése szerinti különleges adatokat és azok hozzávetőleges számát, illetve nagyságrendjét;

d) az adatvédelmi incidensből eredő, valószínűsíthető következményeket;

e) minden, az adatvédelmi incidens megoldására tett vagy tervezett intézkedést, ideértve az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket;

f) az elektronikus információbiztonságot is érintő incidensek esetén az elektronikus információbiztonságért felelős személy által azonosított további kockázatot;

g) az adatvédelmi incidensek kezelése és a kapcsolódó kockázatok mérlegelése tárgyában az Európai Adatvédelmi Testület által elfogadott – vagy a GDPR alkalmazandóvá válását követően fenntartott – iránymutatást;

h) az adatkezelés kapcsán korábban lefolytatott adatvédelmi hatásvizsgálat dokumentációját.

27. § (1) Amennyiben az adatvédelmi tisztviselő úgy ítéli meg, hogy az adatvédelmi incidens valószínűsíthetően kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az adatvédelmi tisztviselő a NAIH honlapjáról letölthető formanyomtatvány alkalmazásával és a GDPR 33. cikk (3) bekezdése szerinti tartalommal bejelenti azt a NAIH felé.

(2) Amennyiben a Szabályzat szerinti vizsgálatot az adatvédelmi tisztviselő véleménye szerint

a) nem lehet 72 órán belül teljeskörűen lefolytatni, vagy

b) nem lehet megállapítani egyértelműen a rendelkezésre álló adatok alapján az adatvédelmi incidenssel érintettek körét, az azzal érintett adatkört, vagy az adatvédelmi incidens bekövetkezésének valamennyi más lényeges körülményét, úgy az adatvédelmi tisztviselő a rendelkezésre álló adatok alapján, szakaszos bejelentést tesz a NAIH részére. A hiányzó adatok megállapítását követően az adatvédelmi tisztviselő intézkedik a teljes bejelentés benyújtása iránt.

28. § (1) Amennyiben az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, vagy az esemény egyéb körülményei alapján az szükséges, a GDPR 34. cikk (3) bekezdésében felsorolt esetek kivételével a szervezeti egység vezetője elrendeli az érintettek tájékoztatását az adatvédelmi incidens kapcsán.

(2) Amennyiben az adatvédelmi incidenssel érintett természetes személyek tájékoztatására – különösen az érintettek köre vagy a kapcsolattartási adatok biztonságának sérülése miatt – észszerű módon nincs lehetőség, úgy az adatvédelmi tisztviselő az adatvédelmi incidens főbb jellemzőire vonatkozó értesítés soron kívüli közzétételét kezdeményezi az Önkormányzat honlapján.

29. § Az adatvédelmi tisztviselő a bekövetkezett adatvédelmi incidensekről a GDPR 33. cikk (5) bekezdése szerint, személyes adatokat nem tartalmazó nyilvántartást vezet, amely tartalmazza

a) az adatvédelmi incidensről készült feljegyzés iktatószámát;

b) az adatvédelmi incidenssel érintett irat vagy nyilvántartás, elektronikus információs rendszer megjelölését vagy azonosítóját;

c) az incidens észlelésének időpontját és a bekövetkezésének megállapított vagy valószínűsített időpontját;

d) az érintett személyes adatok körét;

e) az incidens hatásait, következményeit, valamint az orvoslásukra tett intézkedéseket;

f) a bejelentés időpontját – amennyiben az adatvédelmi incidenst a NAIH részére a GDPR 33. cikk (1) bekezdése szerint bejelentették, vagy annak rövid indokolását, ami miatt az adatvédelmi incidenst nem jelentették be.

VI. Fejezet

AZ ÉRINTETTI JOGGYAKORLÁS BIZTOSÍTÁSÁRA VONATKOZÓ ELŐÍRÁSOK

30. § (1) A szervezeti egységek – a GDPR 5. cikkében foglalt adatkezelési elvek sérelme nélkül, a GDPR 32. cikke szerinti technikai és szervezési intézkedések végrehajtás mellett – az adatkezelésére vonatkozó, érintetti joggyakorlásra irányuló minden beadvány kapcsán – a GDPR 13-14. cikk szerinti tájékoztatás kivételével – esetileg és érdemben vizsgálják azt, hogy elsősorban a kérelmet benyújtó természetes személy kilétével, másodsorban az adatkezelés érintettje azonosításával kapcsolatban merülhetnek-e fel kétségek.

(2) Az érintetti joggyakorlásra irányuló beadvány kapcsán a kérelmet benyújtó természetes személy személyazonosságának megállapítása érdekében további intézkedéseket indokolt tenni különösen, ha az

a) a kérelmező személyének azonosítását nem biztosító elektronikus levélben, elektronikus aláírás nélkül,

b) telefax útján, vagy

c) nem a polgári perrendtartásról szóló 2016. évi CXXX. törvény 325. §-a által meghatározott teljes bizonyító erejű magánokiratba vagy közokiratba foglalt postai küldeményként került megküldésre.

(3) A kérelmet benyújtó természetes személy azonosítása érdekében kizárólag az adott célra szükséges és elégséges többlet személyes adat kérhető. Valamely okiratról készült egyszerű elektronikus másolat, vagy nem hitelesített nem elektronikus másolat megküldése a személy azonosítására nem alkalmas, ezért e célra azok megküldését a kérelmet előterjesztő személytől kétség felmerülése esetén sem lehet kérni.

(4) A szervezeti egység az ellenkező bizonyításáig a kérelmet előterjesztő személy megfelelő azonosításának ismeri el a hitelesített elektronikus aláírással ellátott beadványokat, a teljes bizonyító erejű magánokiratokban foglalt postai úton előterjesztett és az érintett azonosításához szükséges adatokat tartalmazó kérelmeket és a személyazonosság okirattal történő előzetes igazolását követően személyesen előterjesztett beadványokat.

(5) Amennyiben egy érintetti joggyakorlásra irányuló beadvány kapcsán a kérelmet benyújtó természetes személy kilétével kapcsolatban nem merül fel kétség, azonban a kezelt adatok körében megállapítást nyer, hogy az érintett nem azonosítható, – így különösen mert az adatkezelés célja nem teszi szükségessé az érintettnek az azonosítását és bizonyítani tudja, nincs abban a helyzetben, hogy azonosítsa az érintettet – erről haladéktalanul írásban tájékoztatja a kérelmet benyújtó személyt.

(6) Abban az esetben, ha a kérelmet előterjesztő személy megfelelő azonosítására nem alkalmas beadvány érkezik és az abban foglalt – a GDPR 15. cikke szerinti hozzáférési joggyakorlásra, vagy az adatok másolatának kiadására irányuló – kérés olyan adatokra vonatkozik, amelyek megőrzési ideje rövidebb, mint 1 hónap, akkor a kérelmet előterjesztő személy megfelelő azonosítására nem alkalmas kérelemmel érintett adatok kezelését az azonosítást lehetővé tevő kérelem beérkezéséig, de legfeljebb 1 hónapig korlátozza.

(7) Abban az esetben, ha a kérelmet előterjesztő személy megfelelő azonosítására nem alkalmas beadvány érkezik, és abban valamely érintett kapcsolattartási adataira vonatkozó helyesbítéshez való jog gyakorlására irányuló kérelem van, a szervezeti egység hivatalból is köteles vizsgálni, hogy az általa kezelt kapcsolattartási adatok naprakészek-e. A pontosság

elvének történő megfelelés érdekében különösen a kezelt adatok összevetése lehet indokolt a személyiadat- és lakcímnyilvántartásban nyilvántartott adatokkal.

31. § (1) Az érintetti jogok gyakorlására irányuló kérelem elintézésébe az adatvédelmi tisztviselőt be kell vonni. A bármely módon - akár nem hivatalos elérhetőségein keresztül, vagy nem megfelelő módon, esetleg formában - előterjesztett, érintetti joggyakorlásra irányuló kérelmet köteles a az azt fogadó önálló szervezeti egység vezetője soron kívül az adatvédelmi tisztviselő részére is továbbítani.

(2) Az érintetti joggyakorlásra utaló beadványok kapcsán – az adatvédelmi tisztviselő bevonásával – mindenekelőtt meg kell állapítani, hogy abban a GDPR szerinti valamely érintetti jogot, különösen a GDPR 15. cikke szerinti hozzáférési jogot, vagy más, az Ákr. 33-34. §-a szerinti iratbetekintési jogát kívánja-e gyakorolni a beadványozó, esetleg közérdekű adatigénylést kíván-e előterjeszteni.

(3) Az érintetti joggyakorlások teljesítése során a kérelem tárgyában érintett önálló szervezeti egységek közreműködésével vizsgálni szükséges az elektronikus iratkezelő rendszert, és az elektronikus információs rendszereket is.

(4) A szervezeti egység a hozzáférési jog biztosítása során a harmadik fél jogainak védelmét szem előtt tartva jár el az adatokról készített másolat és az azokba történő betekintés biztosítása során is.

32. § (1) A szervezeti egység indokolatlan késedelem nélkül és a lehető legrövidebb időn belül, de legkésőbb az azonosítható érintettől származó kérelem beérkezésétől számított egy hónapon belül tájékoztatja az érintettet a jogai gyakorlására irányuló kérelme nyomán hozott intézkedésekről.

(2) Amennyiben annak a GDPR 12. cikkében foglalt feltételei fennállnak, a válaszadás határideje a szervezeti egység vezetőjének döntése szerint további két hónappal meghosszabbítható, azonban ennek megítélése kapcsán részére az (1) bekezdés szerinti határidőn belül, írásban kell igazolni a késedelem okait, és előterjeszteni a hosszabbítás kapcsán az érintettnek nyújtandó tájékoztatás tervezetét.

(3) A szervezeti egység az érintett részére a kérelmével kapcsolatos tájékoztatást a beadványát figyelembe véve nyújtja, kivételes esetben és arról jegyzőkönyv egyidejű felvétele mellett személyesen is megadhatja.

(4) Az elektronikus úton biztonságosan nem továbbítható személyes adatokat postai úton, tértivevényes küldeményben, elektronikus adathordozón küldi meg az érintett részére, vagy külön kérésére jegyzőkönyv egyidejű felvétele mellett azt személyesen adja át.

VII. Fejezet

KIEGÉSZÍTŐ ÉS ZÁRÓ RENDELKEZÉSEK

Kiegészítő rendelkezések

33. § Amennyiben az Adatkezelő valamely adatkezelésre jogosult dolgozója adatkezeléssel kapcsolatos eljárása során jelen Szabályzat és a vonatkozó jogszabályok alapján sem találja tisztázottnak a követendő eljárást, az adatvédelmi tisztviselőhöz fordulhat. Az adatvédelmi tisztviselő szakmai álláspontja alapján a szervezeti egység vezetője dönt a követendő eljárásról, melyről a szerv dolgozóit szükség esetén egyedileg kiadott utasítás vagy jelen Szabályzat módosítása útján tájékoztatja. Az adatvédelmi tisztviselő köteles jelen Szabályzat szükségszerinti, de legalább évenkénti felülvizsgálatát elvégezni, és a felülvizsgálat eredményeként tett megállapításairól, módosítási javaslatairól a Polgármestereket tájékoztatni.

Záró rendelkezés

34. § Jelen Szabályzat 2026. március 1. napján lép hatályba, és visszavonásig érvényes.

Jóváhagyta:

Zakar Zoltán
polgármester
Apostag Község Önkormányzata

Árizs-Agárdi Bernadett
polgármester
Dunaegyháza Község Önkormányzata