Ügyiratszám: 1560/2018.

A FÜLÖPSZÁLLÁSI POLGÁRMESTERI HIVATAL ADATVÉDELMI ÉS ADATBIZOTONSÁGI SZABÁLYZATA

Adatkezelő Adatvédelmi tisztviselője:
Név: Szabóné dr. Somogyi Szilvia jegyző
Telefonszám: 78/435-322
E-mail: polghivfulop@t-online.hu

A Fülöpszállási Polgármesteri Hivatalnak és a Fülöpszállás Községi Önkormányzatnak (a továbbiakban együtt: Adatkezelő) célja, hogy a tevékenységével összefüggésben felmerülő személyes adatok kezelésével járó folyamatai, eljárásai során biztosítsa a személyes adatok védelmének megfelelő szintjét az Európai Parlament és a Tanács (EU) 2016/679 számú, 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 szóló rendelete szerint (általános adatvédelmi rendelet, vagy Rendelet).

Jelen szabályzat célja, hogy ismertesse az adatok kezelése során érvényesítendő szabályokat és eljárásokat mindazon személyekkel, akik az Adatkezelő adatvagyonához hozzáférhetnek az Adatkezelővel munkavégzésre, adatfeldolgozásra irányuló jogviszonyban állnak.

Az adatkezelési műveleteket Adatkezelő úgy tervezi meg és hajtja végre, hogy az érintettek magánszférájának védelme megfelelő módon biztosított legyen. A technika mindenkori fejlettségére tekintettel — megteszi azokat a technikai és szervezési intézkedéseket és kialakítja azokat az eljárási szabályokat, amelyek az adatbiztonság érvényre juttatásához szükségesek. Az adatokat védi különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, az adatok károsodása és véletlen elvesztése, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen.

Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban Infotv.) 24.§ (3) bekezdésében, valamint a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. törvény (a továbbiakban: Nytv.) 30.§ (1) bekezdésében kapott felhatalmazás alapján az Adatkezelő általános adatvédelmi és adatbiztonsági szabályait az alábbiakban határozom meg.

I. Általános rendelkezések

1.§ A szabályzat célja az Adatkezelő által végzett adatkezelések, adatfeldolgozások során a személyes adatok védelme és közérdekű, illetve közérdekből nyilvános adatok hozzáférhetőségének biztosítása.

2.§ A szabályzat tárgyi hatálya – figyelemmel az Infotv. 2.§-ában foglaltakra – kiterjed az Adatkezelő által folytatott minden olyan adatkezelésre és adatfeldolgozásra, amely természetes személy adataira vonatkozik, valamint amely közérdekű adatot vagy közérdekből nyilvános adatot tartalmaz, függetlenül attól, hogy az adatkezelés, adatfeldolgozás teljesen vagy részben automatizált eszközzel, valamint manuális módon történik.

3.§ A szabályzat hatálya nem terjed ki:

a) Az Informatikai Biztonsági Szabályzatban rendezett kérdésekre,
b) az Adatkezelő munkavégzésre irányuló jogviszonnyal kapcsolatos adatkezelési tevékenységére, csak amennyiben az ilyen tárgyú szabályzat e szabályzatra visszautal.
c) az anonim információkra, nevezetesen olyan információkra, amelyek nem azonosított vagy azonosítható természetes személyekre vonatkoznak, valamint az olyan személyes adatokra, amelyeket olyan módon anonimizáltak, amelynek következtében az érintett nem, vagy többé nem azonosítható;
d) az elhunyt személyekkel kapcsolatos személyes adatok kezelésére.

4.§ A szabályzat személyi hatálya kiterjed az önkormányzat tisztségviselőire, az Adatkezelő által foglalkoztatott valamennyi köztisztviselőre, ügykezelőre, a munka törvénykönyve hatálya alá tartozó munkavállalóira és a munkavégzésre irányuló egyéb jogviszonyban álló személyekre, valamint az adatfeldolgozási szerződésekben rögzítettek szerint, az adatfeldolgozási szerződést aláírt külső szervezetek mindazon alkalmazottaira, akik az Adatkezelő informatikai rendszereit használják, üzemeltetik, működtetik vagy fejlesztik – azaz mindazon személyekre, akik az Adatkezelő adatvagyonához hozzáférhetnek (a továbbiakban: alkalmazott).

5.§ Az értelmező rendelkezések tekintetében az Infotv. 3.§-a az irányadó.

6.§ A személyes adatok védelméhez fűződő jogot és az érintett személyiségi jogait, ha törvény kivételt nem tesz, az adatkezeléshez fűződő más érdek – ideértve a közérdekű adatok nyilvánosságát is – nem sérthetik.

II. Az adatkezelés jogalapjai és korlátai

7.§ Személyes adat főszabály szerint két esetben kezelhető:

a) ha az érintett hozzájárul az adatkezeléshez – ebben az esetben az Adatkezelőnél mindaddig, amíg az a személyes adatokat kezeli, rendelkezésre kell állni az érintett kifejezett írásbeli hozzájáruló nyilatkozatának-,
b) vagy törvény vagy – törvényi felhatalmazás alapján, az abban meghatározott körben – helyi önkormányzat rendelete közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges adatkezelést rendel el.

c) További jogalapok:

1. 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,

2. az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges,

3. az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges.

8. § Különleges adatok kezelésével járó ügyekben a jelen szabályzatban foglaltakon túl is megkülönböztetett gondossággal kell eljárni. Figyelemmel kell lenni arra, hogy különleges adatok kizárólag törvényi (illetve a rendeletbeli) felhatalmazás alapján, illetve az érintett írásbeli hozzájárulásával kezelhetőek.

9. § Az adatkezelő adatkezelési tájékoztatással kapcsolatos kötelezettségei:

a) Az újonnan megkezdett adatkezelés esetében

1. amennyiben az érintettre vonatkozó személyes adatokat az Adatkezelő az érintettől gyűjti, a személyes adatok megszerzésének időpontjában,

2. amennyiben az érintett utólag kér tájékoztatást, úgy ezen tájékoztatás megadásakor is

b) az érintett rendelkezésére kell bocsátani az alábbi információkat:

1. az Adatkezelő és – amennyiben ilyen kijelölésre kerül – képviselőjének kiléte és elérhetőségei,

2. az adatvédelemért felelős személy elérhetőségei,

3. a személyes adatok tervezett kezelésének célja, valamint az adatkezelés jogalapja (ideértve különösen az Adatkezelő és harmadik fél jogos érdekeinek kifejtését is),

4. a személyes adatok címzettjei, amennyiben van ilyen, a címzettek kategóriái,

5. adott esetben annak a ténye, ha az Adatkezelő harmadik országba, vagy nemzetközi szervezet részére kívánja az adatokat továbbítani, a vonatkozó megfelelőségi határozat léte vagy hiánya, vagy ilyen adattovábbítás esetén megfelelő és alkalmas garanciák megjelölése, valamint azok másolatának megszerzésére szolgáló módokra vagy azok elérhetőségére való hivatkozás,

6. a személyes adatok tárolásának időtartama, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjai,

7. az érintett azon jogáról történő tájékoztatása, hogy kérelmezheti az Adatkezelőtől a rá vonatkozó személyes adatokhoz való hozzáférést, azok helyesbítését, törlését vagy

kezelésének korlátozását (zárolás) és tiltakozhat az ilyen személyes adatok kezelése ellen, valamint az érintett adathordozhatósághoz való jogát,

8. amennyiben az adatkezelés az érintett hozzájárulásán alapul, az arról való tájékoztatást, hogy hozzájárulását bármely időpontban visszavonhatja, amely nem érinti a visszavonás előtt a hozzájárulás alapján végrehajtott adatkezelés jogszerűségét,

9. az érintettnek joga van felügyeleti hatósághoz címzett panasz benyújtására,

10. azt, hogy a személyes adat szolgáltatása jogszabályon vagy szerződéses kötelezettségen alapul vagy szerződés kötésének előfeltétele-e, valamint, hogy az érintett köteles-e személyes adatokat megadni továbbá, hogy milyen lehetséges következményekkel járhat az adatszolgáltatás elmaradása,

11. amennyiben ez releváns, az automatizált döntéshozatal ténye, ideértve a profilalkotást is, valamint legalább ezekben az esetekben az alkalmazott logikára és arra vonatkozó közlés, hogy az ilyen adatkezelés milyen jelentőséggel és az érintettre nézve milyen várható következményekkel bír.

c) Az újonnan megkezdett adatkezelés esetében amennyiben erre lehetőség van, továbbá ha az érintettre vonatkozó személyes adatokat az Adatkezelő nem az érintettől gyűjti, a személyes adatok megszerzésének időpontjában, illetőleg a tájékoztató elkészítésekor az érintett rendelkezésére bocsátja a fenti információkat, valamint a személyes adatok forrását és adott esetben azt, hogy az adatok nyilvánosan hozzáférhető forrásból származnak-e.

10. § A személyes adatok kezelése célhoz kötöttségének elve alapján az egyes eljárások során kezelt adatokat csak az adott ügy elintézése érdekében szabad felhasználni, más eljárásokkal, illetve adatokkal azok nem kapcsolhatók össze, kivéve, ha törvény megengedi, illetve az érintett hozzájárult és az adatkezelés feltételei minden egyes személyes adatra vonatkozóan fennállnak.

11. § Konkrét ügyben hivatalból csak azokat a személyes adatokat lehet rögzíteni, amelyek kezelésére törvény vagy törvény felhatalmazása alapján, az abban meghatározott körben önkormányzati rendelet, illetve az érintett felhatalmazást ad, mellőzve a bemutatott személyazonosító és egyéb okmányok, személyes iratok indokolatlan fénymásolását és megőrzését.

12. § Amennyiben az Adatkezelő a személyes adatokon a gyűjtésük céljától eltérő további célból adatkezelést kíván végezni és erre lehetősége van, a Rendelet vonatkozó szabályaira tekintettel a további adatkezelést megelőzően tájékoztatja az érintettet erről az eltérő célról és minden, a fenti pontokban megfogalmazott információról.

13. § Az adatminőség biztosítása céljából az adatfelvétel és a további adatkezelés folyamán ügyelni kell a személyes adatok felvételének és kezelésének törvényességére, pontosságára, teljességére és – amennyiben az adatkezelés céljára tekintettel szükséges – időszerűségére, megfelelő tárolására, hogy emiatt az érintettek jogai ne sérülhessenek.

14. § A célhoz nem kötött és olyan adatokat, amelyekre nézve az adatkezelés célja megszűnt vagy módosult – az Iratkezelési Szabályzatban foglaltakkal összhangban – haladéktalanul, illetve az előírt megőrzési határidő leteltével meg kell semmisíteni. A személyes adatokat tartalmazó egyéb iratanyagok megsemmisítéséről szintén a szükséges biztonsági intézkedések mellett kell gondoskodni. Az elektronikus úton rögzített adatokat, ha céljukat betöltötték további felhasználásuk megakadályozása érdekében felismerhetetlenné, hozzáférhetetlenné kell tenni.

15. § Az adattörlés maradéktalan megvalósítása érdekében az irattározásra kerülő anyagok selejtezési idejét, irattári jelét az Adatkezelő Iratkezelési Szabályzatának mellékletét képező Irattári Terv határozza meg.

16. § Adatkezelő továbbá törli vagy anonimizálja az érintettre vonatkozó, az informatikai rendszereiben, valamint papír alapú dokumentációiban szereplő személyes adatokat, ha jogszabály máshogy nem rendelkezik és a személyes adat kezeléséhez fűződő cél megszűnt. Amennyiben a személyes adat törlése nem valósítható meg, az azt tartalmazó irat sérelme nélkül:

a) amennyiben az irat megőrzéséhez az Adatkezelő, vagy harmadik személy jogos érdeke fűződik, az iratot az Adatkezelő az iratkezelési szabályok szerinti időtartamig megőrzi, törlési kérelem esetén az iratot zártan kezeli és erről az érintettet értesíti, és az iratot a személyes adattal együtt az Iratkezelési Szabályban meghatározott időtartam lejártát követően megsemmisíti,

b) amennyiben az irat megőrzéséhez az Adatkezelőnek és harmadik személynek sem fűződik jogos érdeke, az iratot a személyes adattal együtt megsemmisíti.

17. § Az adatok törlése iránt minden esetben az adatvédelemért felelős személy a személyes adat kezelésével kapcsolatban érintett szervezeti egységgel, informatikai rendszer rendszergazdájával együttműködésben intézkedik. Az Adatkezelő informatikai rendszereiből a személyes adatot – az adott informatikai rendszer adottságai szerint – az élő rendszerből visszaállíthatatlanul törli vagy anonimizálja, továbbá az elérhető technológia és a megvalósítás költségeinek figyelembevételével megteszi az elvárható lépéseket és gondoskodik arról, hogy az informatikai rendszer archivált változatában is – a technológiai, technikai lehetőségek függvényében – átvezetésre kerüljön a személyes adat törlése. A törlésért az informatikai rendszerért felelős személy felel. Amennyiben a helyreállíthatatlan törlés informatikai rendszer sajátosságából következő okból nem kivitelezhető, Adatkezelő az adat logikai törlését hajtja végre. Az anonimizálás keretében a személyes adatot olyan azonosítóra kell lecserélni, amely megakadályozza, hogy a személyes adathoz tartozó további adatok a későbbiekben kapcsolatba hozhatók legyenek az érintettel. A papír alapú dokumentációk esetében azok jegyzőkönyvvel rögzített megsemmisítéséről kell gondoskodni. A jegyzőkönyvben rögzíteni kell: a megsemmisített iratok típusát, a megsemmisített iratok beazonosíthatóságához szükséges információkat, a megsemmisítés időpontját és a megsemmisítést végző személy nevét, beosztását, külső partner esetén a külső partner nevét.

18. § A személyes adatok akkor továbbíthatók, valamint a különböző adatkezelések akkor kapcsolhatók össze, ha az érintett ahhoz hozzájárult, vagy törvény azt megengedi, és ha az adatkezelés feltételei minden egyes személyes adatra nézve teljesülnek. Személyes adat (beleértve a különleges adatot is) az országból – az adathordozótól vagy az adatátvitel módjától függetlenül – harmadik országban lévő adatkezelő vagy adatfeldolgozó részére akkor továbbítható, ha az Infotv. 8. §-ában foglalt feltételek teljesülnek.

19. § A hatósági ügyek során hozott döntések nem tartalmazhatják az értesítendő személyek és szervek nevét, címét. Annak érdekében, hogy a kézbesítés ellenőrizhető legyen, a köztisztviselő köteles az irattári példányon rögzíteni az értesítendők jegyzékét, arról tájékoztatást adni azonban csak a vonatkozó jogszabályok és jelen szabályzat rendelkezéseinek figyelembevételével lehet.

III. Az érintett jogai

20. § Az érintettet a törvény szerint megilleti az a jog, hogy személyes adatai kezeléséről tájékoztatást kérjen.

A jelen pont szerinti tartalmú kérelmet (a jogszabályi feltételek fennállása esetén) a törvény alapján legfeljebb 30 napon belül, lehetőség szerint azonban soron kívül teljesíteni kell. A tájékoztatásnak az Infotv. 15. § (1) bekezdése szerinti adatokat kell tartalmaznia. A tájékoztatás ingyenes, ha a tájékoztatást kérő a folyó évben azonos adatkörre vonatkozóan tájékoztatási kérelmet még nem nyújtott be. Egyéb esetben I FŐJEGYZŐ/LEÁS Polgármesteri Hivatalának a közérdekű adatok megismerésére irányuló igények teljesítésének rendjéről szóló szabályzatban meghatározott díjak az irányadók. A már megfizetett költségtérítést vissza kell téríteni, ha az adatokat jogellenesen kezelték vagy a tájékoztatás kérése helyesbítéshez vezetett.

A tájékoztatás az adott adatkezelésről készült tájékoztatóban megjelölt elektronikus e-mail címen vagy postai levélben kérhető. A tájékoztatást az érintett által kért formában kell megadni, erre irányuló kifejezett kérés hiányában elsősorban emailen keresztül, másodsorban postai küldeményként kell megadni, amennyiben az Adatkezelő számára rendelkezésre áll a kommunikációs forma használatához szükséges adat és amennyiben az érintett személyazonossága kétséget kizáróan megállapítható.

A tájékoztatás keretében az adatvédelemért felelős személy – vagy a szerződésben erre a feladatra kijelölt adatfeldolgozó – köteles az érintettre vonatkozó, Adatkezelő által kezelt adatokról és a fentiekről tájékoztatást adni.

21. § Az Adatkezelő az érintett kérelmére köteles arra, hogy az érintettre vonatkozó személyes adatokat indokolatlan késedelem nélkül, de legfeljebb 30 napon belül törölje, ha az alábbi indokok valamelyike fennáll:

a) a személyes adatokra már nincs szükség abból a célból, amelyekből azokat gyűjtötték vagy más módon kezelték,

b) az érintett visszavonja az adatkezelés alapját szolgáló hozzájárulását és az adatkezelésnek más jogalapja nincs,

c) az érintett a közérdekű, valamint az Adatkezelő vagy harmadik fél jogos érdekeinek érvényesítéséhez szükséges adatkezelés ellen tiltakozik és nincs elsőbbséget élvező jogszerű ok az adatkezelésre, vagy az érintett a közvetlen üzletszerzés céljából beszerzett adatainak kezelése ellen tiltakozik,

d) a személyes adatokat jogellenesen kezelte az Adatkezelő,

e) a személyes adatokat az Adatkezelőre alkalmazandó uniós vagy tagállami jogban előírt jogi kötelezettség teljesítéséhez törölni kell,

f) a személyes adatok gyűjtésére a Rendelet szerinti, információs társadalommal összefüggő szolgáltatások kínálásával kapcsolatosan került sor.

Amennyiben az Adatkezelő nyilvánosságra hozta a személyes adatot és azt törölni köteles, az elérhető technológia és a megvalósítás költségeinek figyelembevételével megteszi az ésszerűen elvárható lépéseket – ideértve technikai intézkedéseket – annak érdekében, hogy tájékoztassa az adatokat kezelő Adatkezelőket, hogy az érintett kérelmezte tőlük a szóban forgó személyes adatokra mutató linkek vagy e személyes adatok másolatának, illetve másodpéldányának törlését.

22. § A törlést nem kell teljesíteni amennyiben az adatkezelés

a) véleménynyilvánítás szabadságához vagy a tájékoztatáshoz való jog gyakorlása céljából szükséges,

b) jogi igények előterjesztéséhez, érvényesítéséhez és védelméhez szükséges,

c) jogi kötelezettség teljesítése miatt szükséges,

d) közérdekű archiválás, tudományos vagy történelmi kutatás, statisztikai célból szükséges és az adattörlés lehetetlenné tenné, vagy komolyan veszélyeztetné az adatkezelés céljának teljesítését,

e) az informatikai rendszerek konzisztens, jogszerű működésének fenntartása érdekében szükséges.

Amennyiben az adatok törlése jogszabályi előírás, de az az érintett jogos érdeke miatt nem lehetséges, a személyes adatot, illetve a személyes adatot tartalmazó elektronikus vagy papír alapú dokumentációt zárolni kell. Ez esetben az informatikai rendszerben tárolt adathoz, illetve dokumentumhoz csak az informatikai rendszer rendszergazdája vagy az adatvédelemért felelős személy rendelkezhet hozzáféréssel. Papír alapú dokumentációk esetén pedig a dokumentum őrzését zárható szekrényében kell megvalósítani.

A papír alapú dokumentációk belső rendszerbe feltöltött elektronikus példányához az Adatkezelő a felhasználók hozzáférését megszünteti.

23. § Az érintett bármikor jogosult a helytelenül rögzített adatainak helyesbítését kérni. Amennyiben az érintett jelzi, hogy az Adatkezelő által kezelt bármely adata nem felel meg

a valóságnak, az adatvédelemért felelős személy azonosítja az érintettet, valamint az általa helyesbítésre kért adat nyilvántartás helyét, és gondoskodik az adat helyesbítéséről, ezen eljárása keretében az adat helyesbítésére vonatkozó igényt az Adatkezelő érintett informatikai rendszerének rendszergazdája felé jelzi, a szükséges azonosító adatok, a hibás és a helyes adat megadásával. Amennyiben a helyes adat nem áll rendelkezésre, az adatvédelemért felelős személy az érintettől kér felvilágosítást a helyes adatról. Ha a helyes adat nem állapítható meg, az adatvédelemért felelős személy gondoskodik a helytelen adat zárolásáról. A zárolás az adat passzív állapotba helyezését jelenti, valamint értesíti az érintetett, hogy az adat helyesbítésére a helyes adat hiányában nincs mód, de az adat zárolásra került. Az eljárás határideje 30 nap.

24. § Az érintett jogosult arra, hogy tiltakozzon személyes adatának kezelése ellen. Az adatvédelemért felelős személy a legrövidebb időn belül azonosítja az érintettet, a tiltakozást a kérelem benyújtásától számított legrövidebb időn belül megvizsgálja, annak megalapozottsága kérdésében döntést hoz és döntéséről a kérelmezőt tájékoztatja.

25. § Az érintett jogosult arra, hogy kérésére Adatkezelő korlátozza az adatkezelést, ha az alábbiak valamelyike teljesül:

a) az érintett vitatja a személyes adatok pontosságát, ez esetben a korlátozás arra az időtartamra vonatkozik, amely lehetővé teszi, hogy az Adatkezelő ellenőrizze a személyes adatok pontosságát;

b) az adatkezelés jogellenes, és az Adatkezelő ellenzi az adatok törlését és e helyett kéri azok felhasználásának korlátozását;

c) Adatkezelőnek már nincs szüksége a személyes adatokra adatkezelés céljából, de az érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez; vagy

d) az érintett tiltakozott az adatkezelés ellen, de az Adatkezelő jogos érdeke is megalapozhatja az adatkezelést, ez esetben amíg megállapításra nem kerül, hogy az Adatkezelő jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben, az adatkezelést korlátozni kell.

Ha az adatkezelés korlátozás alá esik, az ilyen személyes adatokat a tárolás kivételével csak az érintett hozzájárulásával, vagy jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez, vagy más természetes vagy jogi személy jogainak védelme érdekében, vagy az Unió, illetve valamely tagállam fontos közérdekéből lehet kezelni.

Adatkezelő az érintettet, akinek a kérésére korlátozták az adatkezelést, az adatkezelés korlátozásának feloldásáról előzetesen tájékoztatja.

26. § A panaszok kezelésével kapcsolatban az adatvédelemért felelős személy számára tájékoztatást kötelesek adni a személyes adatok kezelésében részt vevő munkavállalók, egyéb személyek.

27. § Ha az Adatkezelő bizonyítani tudja, hogy nincs abban a helyzetben, hogy azonosítsa az érintettet, erről lehetőség szerint őt megfelelő módon tájékoztatja. Ilyen esetekben az érintett hozzáférési jogát, a helyesbítés és törlés kérésének jogát, az adatkezelés korlátozásához való jogát, az ezekhez kapcsolódó értesítési jogot, valamint adathordozhatósához való jogot az Adatkezelő nem biztosítja, kivéve, ha az érintett abból a célból, hogy az említettek szerinti jogát gyakorolja, az azonosítását lehetővé tevő kiegészítő információkat nyújt.

IV. Az adatvédelmi tisztviselő

28. § Az adatvédelmi tisztviselőt az adatvédelmi jog és gyakorlat szakértői szintű ismerete, valamint az e §-ban említett feladatok ellátására való alkalmasság alapján kell kijelölni. Az Adatkezelő adatvédelmi tisztviselőjét a jegyző nevezi ki.

29. § Az adatvédelmi tisztviselő elektronikus elérhetőségét közzéteszi. Az adatvédelmi tisztviselőhöz bármely érintett fordulhat. Az adatvédelmi tisztviselő feladatait az adatkezelési műveletekhez fűződő kockázat megfelelő figyelembevételével, az adatkezelés jellegére, hatókörére, körülményére és céljára is tekintettel végzi. Az adatvédelmi tisztviselő

a) közreműködik, illetve segítséget nyújt az adatkezeléssel összefüggő döntések meghozatalában, valamint az érintettek jogainak biztosításában,

b) ellenőrzi az információs önrendelkezési jogról és az információszabadságtól szóló 2011. évi CXII. törvény, a Rendelet, az adatkezelésre vonatkozó ágazati jogszabályok, valamint a szabályzat előírásai és az adatbiztonsági követelmények teljesülését, a tapasztalatokról és az esetleges hiányosságok megszüntetése érdekében teendő intézkedésekről tájékoztatja az érintett szervezeti egység vezetőjét és a jegyzőt,

c) kivizsgálja és intézi a hozzá érkező bejelentéseket,

d) a b)-c) pontokban körülírt vagy egyéb módon tudomására jutott visszásság esetén hivatalon belül felhívja az érintett alkalmazottat a jogosultatlan vagy nem megfelelő adatkezelés megszüntetésére,

e) rendszeresen felülvizsgálja az adatvédelmi szabályzatot, figyelemmel kíséri a hatályosulását, jogszabály változás miatt vagy más fontos okból gondoskodik módosításáról, kiegészítéséről,

f) vezeti a belső adatvédelmi nyilvántartást és összesíti, majd a kitűzött határidőre továbbítja a Nemzeti Adatvédelmi és Információszabadság Hatóság részére az Infotv.-ben előírt éves jelentést,

g) a közérdekű adatok nyilvánosságával kapcsolatban szükség szerint közreműködik a közvélemény tájékoztatásában és a hasonló adatok megismerése iránti kérelmek teljesítésében,

h) igény szerint tájékoztatja a jegyzőt a konkrét ügyek vagy jelentősebb soron kívüli feladatok végrehajtásáról, tapasztalatairól,

i) részt vesz az adatvédelmi tisztviselők konferenciáján.

j) Az adatvédelmi tisztviselő az adatkezelések átláthatóságának biztosítása érdekében nem nyilvános adatvagyon nyilvántartást vezet, amely tartalmazza legalább:

1. az adatkezelési eset megnevezését,
2. az Adatkezelő kezelésében lévő adatok felsorolását,
3. azt, hogy adott adat milyen informatikai rendszerben kerül kezelésre,
4. az adatkezelés célját,
5. az adatkezelés időtartamát,
6. az adatfeldolgozók személyét,
7. az adat forrását,
8. az adatkezelési folyamat adatgazdája szervezeti egységét, személyét,
9. adatfeldolgozás esetén az adatfeldolgozó nevét és elérhetőségeit.

k) Az érintettek jogainak biztosítása körében:

1. Az adatvédelmi tisztviselő hatékony eljárásokat dolgoz ki annak érdekében, hogy az érintettek egyszerűen tudják a jogaikat gyakorolni vagy az általuk észlelt jogsértés miatt bejelentést tenni.
2. Az adatkezeléssel kapcsolatban érkezett panaszok, bejelentések kivizsgálása során az adatvédelmi tisztviselő jár el.
3. Amennyiben a panasz vagy bejelentés kivizsgálása arra okot adó körülményeket tárt fel, az adatvédelmi tisztviselő a panasztevő vagy bejelentő egyidejű tájékoztatása mellett adatvédelmi intézkedések megtételére, azok kezdeményezésére jogosult.

l) Adatvédelmi és adatbiztonsági követelmények érvényesítése, azok megtartásának ellenőrzése körében az adatvédelmi tisztviselő az adatkezelését meghatározó jelen szabályzatban hivatkozott és egyéb vonatkozó jogszabályok, belső adatvédelmi és adatbiztonsági szabályzatok rendelkezéseinek és az adatbiztonsági követelmények megtartását folyamatosan ellenőrzi, ideértve feladatkörök kijelölését, az adatkezelési műveletekben résztvevő személyek tudatosság-növelését és képzését, valamint a kapcsolódó auditokat is.

m) Az Adatkezelő adatkezelési tevékenységével összefüggő döntések meghozatalában való közreműködése körében:

1. Az adatvédelmi tisztviselő figyelemmel kíséri a jogszabályi rendelkezések gyakorlati alkalmazhatóságát, szükség esetén javaslatot tesz az egyes adatkezelési körülmények megváltoztatására vagy kiegészítésére.

2. Közreműködik a szükséges jogszabály-módosítások előkészítésében.

3. Az adatkezelést érintő tervezett döntéssel kapcsolatban, a döntés meghozatalát megelőzően ki kell kérni az adatvédelmi tisztviselő véleményét. A vélemény kérésével egy időben tájékoztatni kell legalább a döntés körülményeiről, hatásáról, döntési alternatívákról. A tájékoztatást olyan időben kell az adatvédelmi tisztviselő részére eljuttatni, hogy megfelelő idő álljon rendelkezésére álláspontja kialakítására. Az adatvédelmi tisztviselő a döntéssel kapcsolatos álláspontját a döntés meghozatalát megelőzően juttatja el a döntés előkészítőinek. A döntéshozatal során az adatvédelmi tisztviselő véleményét figyelembe kell venni.

n) Az adatbiztonsági incidensek kezelése során való eljárása körében:

1. Adatvédelmi incidensek kezelése érdekében az adatvédelmi tisztviselő jár el. Az incidens kezelése során az adatvédelmi tisztviselő tájékoztatást ad az adatkezelő által kezelt, illetve a megbízott adatfeldolgozó által feldolgozott adatokról, azok forrásáról, az adatkezelés céljáról, jogalapjáról, időtartamáról, az adatfeldolgozó nevéről, címéről és az adatkezeléssel összefüggő tevékenységéről; az adatvédelmi incidens körülményeiről, hatásairól és az elhárítására megtett intézkedésekről; az érintett személyes adatainak továbbítása esetén az adattovábbítás jogalapjáról és címzettjéről.

2. Az adatvédelmi tisztviselő vezeti az adatvédelmi incidenssel kapcsolatos intézkedések ellenőrzése, valamint az érintett tájékoztatása céljából az adatvédelmi incidensekre vonatkozó, 1. melléklet szerinti nyilvántartást.

o) Adatvédelmi ismeretek oktatása, terjesztése körében

1. vezető tisztségviselők, alkalmazottak részére az adatvédelemmel kapcsolatos feladataikra és kötelezettségeikre kiterjedő rendszeres oktatást szervez, a Rendelet által meghatározott kötelezettségekkel kapcsolatban tájékoztatást, illetve szakmai tanácsot ad,

2. az Adatkezelő adatkezelésével kapcsolatos gyakorlat megváltozása esetén az tájékoztatást ad mindazok részére, akikre a változás hatással lehet,

3. gondoskodik az adatkezelést végző munkatársak adatvédelmi ismereteinek naprakészen tartásáról,

4. kérésre szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, valamint nyomon követi a hatásvizsgálatnak a Rendelet 35. cikkében foglaltak szerinti elvégzését.

V. Adatfeldolgozó igénybevétele

30. § Az Adatkezelő adatfeldolgozó igénybevétele esetén gondoskodik arról, hogy a kiválasztott adatfeldolgozó a személyes adatok védelme érdekében megtegye a szükséges intézkedéseket, valamint kövesse Adatkezelő szabályzatait és egyedi utasításait. A kiválasztás során az Adatkezelő törekszik arra, hogy csakis olyan adatfeldolgozó kerüljön igénybevételre, amely megfelelő garanciákat nyújt – különösen szakértelem, megbízhatóság és erőforrások tekintetében – arra vonatkozóan, hogy az adatvédelmi követelmények teljesülését biztosító technikai és szervezési intézkedéseket végrehajtja, ideértve az adatkezelés biztonságát is.

31. § A szabályzat hatálybalépését követően kötött adatfeldolgozói szerződésekben legalább az alábbiakról rendelkezni kell:

a) szerződés tárgya,

b) az Adatkezelő és az adatfeldolgozó adatai,

c) a feldolgozott adatok körének megjelölése,

d) az adatfeldolgozás céljai,

e) az adatfeldolgozás időtartama,

f) a feldolgozandó személyes adatok becsült mennyisége,

g) az adatfeldolgozó által elvégzett technikai műveletek megnevezése és alapvető elemei;

h) az érintettek köre,

i) adatfeldolgozó által ellátandó feladatok pontos leírása,

j) az utasításhoz kötöttség ténye,

k) a tájékoztatási kötelezettséget,

l) arról, hogy az adatfeldolgozó a Rendeletben alkalmazott biztonsági eljárásokra (álnevesítés, titkosítás) felkészül, azokat legkésőbb a Rendelet alkalmazásának megkezdésétől bevezeti,

m) Adatkezelő rendszergazdájának, információbiztonsági felelősének és adatvédelemért felelős személyének elérhetősége,

n) adatfeldolgozó titoktartási kötelezettsége,

o) az adatkezelés jellegének figyelembevételével megfelelő technikai és szervezési intézkedések meghatározása, az adatbiztonsági előírások meghatározása,

p) annak meghatározása, hogy az adatfeldolgozónak az Adatkezelő mely szabályzatainak kell megfelelnie,

q) további adatfeldolgozó igénybevételének lehetőségét, amennyiben ez ismert, a további adatfeldolgozó személyének megjelölésével, amennyiben nem ismert a bevonás menetére vonatkozó rendelkezéseket és az Adatkezelő ellenvetési jogát,

r) a további adatfeldolgozónak megfelelő garanciákat kell nyújtania a megfelelő technikai és szervezési intézkedések végrehajtására, és ezáltal biztosítania kell, hogy az adatkezelés megfeleljen a Rendelet követelményeinek,

s) az adatfeldolgozás befejezését követő eljárásokat (minden személyes adatot törölni kell vagy vissza kell juttatni az Adatkezelő számára és törölni kell a meglévő másolatokat, kivéve, ha az uniós vagy a tagállami jog az személyes adatok tárolását írja elő),

t) a további adatfeldolgozóval az adatfeldolgozónak az eredeti szerződésének megfelelő tartalmú szerződést kell kötnie,

u) az együttműködés elvét azaz, hogy az adatfeldolgozónak kötelessége az Adatkezelővel együttműködni az alanyi jogok teljesítési során,

v) az Adatkezelő és az adatfeldolgozó közötti utasításadás, illetve kapcsolattartás módja,

w) a felelősség elvét, azaz annak tényét, hogy az Adatkezelő az adatfeldolgozó rendelkezésére bocsát minden olyan információt, amely az Adatkezelő Rendeletben megfogalmazott kötelezettségeinek teljesítéséhez szükséges,

x) az audit jog kikötését azaz, hogy az adatfeldolgozó köteles elősegíteni az Adatkezelő által vagy az általa megbízott más természetes vagy jogi személy által végzett auditokat, beleértve a helyszíni ellenőrzéseket,

y) a felelősség egyes kérdései a felek között,

z) jogérvényesítési lehetőségek a felek között.

VI. Adatbiztonsági rendelkezések

Általános szabályok

32. § Valamennyi alkalmazott köteles:

a) az Infotv. és az ágazati jogszabályok, valamint jelen szabályzat adatvédelmi előírásait megismerni és betartani,

b) indokolt esetben előzetesen egyeztetni az adatvédelmi felelőssel a személyes adatok kezelését vagy a közérdekű adatok nyilvánosságát érintő ügyekben, tájékoztatni a

feladatkörében felmerült bármely egyéb ágazati adatvédelmi problémáról, esetleges állásfoglalásról vagy más fejleményről, észrevételezés esetén az adatkezeléssel kapcsolatosan feltárt visszásságot jelezni,

c) az éves adatvédelmi jelentéshez felettes vezetője útján adatot szolgáltatni.

A munkavégzés szabályai

33. § Az alkalmazottak irodai helyiségüket és az irat és adattárolásra használt berendezéseket munkaidőben fokozott gondossággal kötelesek őrizni. Az alkalmazott köteles a számítógépét és az ahhoz alkalmazott adathordozókat úgy kezelni, tárolni, hogy a védelmet igénylő adatokat illetéktelen személy ne ismerhesse meg. Köteles továbbá a munkaidő végeztével a számítógépet kikapcsolni, az irodahelyiség ajtaját bezárni és a kulcsot a portaszolgálathoz leadni.

34. § Személyes adatokat is tartalmazó iratot vagy más adathordozót (a továbbiakban együtt: irat) az Adatkezelő helyiségeiből kivinni – munkaköri feladat ellátásának kivételével – csak indokolt esetben, a felettes vezető egyetértésével lehet. Az alkalmazott ez esetben is köteles gondoskodni arról, hogy az irat ne vesszen el, ne rongálódjon vagy semmisüljön meg és tartalma illetéktelen személy tudomására ne jusson.

35. § Az alkalmazott a nála lévő iratokat köteles munkaidőn túl – és amelyeket lehetséges munkaidőben is – elzárt helyen tartani. Munkaidőben iratok csak a munkavégzés céljából és a munkavégzéshez szükséges időtartamban lehetnek a köztisztviselőnél.

36. § A közgyűlési, bizottsági és települési kisebbségi önkormányzati jegyzőkönyvek közül a zárt ülések jegyzőkönyveit fokozott gondossággal kell kezelni. A zárt ülések jegyzőkönyveit külön kell lefűzni vagy beköttetni, zárható szekrényben kell tárolni.

37. § Akár alkalmazottnál, akár irattárban lévő iratba az ügyintéző alkalmazotton kívül más személy – a vonatkozó eljárásjogi szabályok szerint – csak akkor tekinthet be, ha ezt jogszabály lehetővé teszi. A betekintési jog gyakorlása során úgy kell eljárni, hogy ez által mások személyes adatainak védelméhez fűződő jogai, illetve személyiségi jogai ne sérülhessenek. Jelen pont rendelkezéseit kell alkalmazni a másolat, kivonat készítésekor is.

38. § Az ügyfélfogadáshoz az alkalmazottak részére lehetőség szerint külön szobát kell biztosítani.

39. § Az egyes nyilvántartások, adatkezelések tekintetében a hozzáférési jogosultságot az illetékes szervezeti egység vezetőjének személyre szólóan meg kell határoznia és az időszerű állapotnak megfelelően a rendszergazdának nyilván kell tartania az Jogosultságkezelési Szabályzatban foglaltak szerint.

40. § Az alkalmazottak a munkavégzés, illetve feladatellátás során keletkezett személyes adatot is tartalmazó elektronikus dokumentumokat csak a munkavégzés céljára szolgáló számítástechnikai eszközökön nyithatják meg. Továbbá:

a) A munkavégzésre, illetve feladatellátásra használt eszközt, amelyen az Adatkezelő által kezelt vagy feldolgozott személyes adat is megtalálható, minden esetben ábrás, vagy kódos védelemmel kell használni. Az alkalmazott köteles a Munkáltató által biztosított készüléken képernyőzárat – ábrát, vagy kódot – létrehozni, továbbá a készüléket folyamatosan ábrás vagy kódos védelemmel ellátva használni, melyet kizárólag az alkalmazott ismer. A hozzáférési kódokat az alkalmazottak bizalmasan kötelesek kezelni. Az alkalmazott köteles a kódot az eszköz visszaadásának napján az Adatkezelő számara megadni vagy az eszközt kóddal nem védett állapotban visszaszolgáltatni.

b) A munkavégzés/feladatellátás céljára szolgáló eszközökön a személyes adatot is tartalmazó dokumentumot az alkalmazottak nem nyithatják meg. Amennyiben valamely okból ez elkerülhetetlen, akkor a helyi másolatot minden esetben törölni kell az eszközről.

c) A munkavégzés, illetve feladatellátás céljára átadott eszközöket kizárólag az alkalmazottak használhatják, hozzátartozóik vagy más személy számára nem engedélyezett a használat.

Személyes adatok kezelésére vonatkozó különös rendelkezések

41. § A papír alapú, személyes adatokat tartalmazó munkadokumentumokat olyan módon kell kezelni, tárolni, hogy azokat csak az erre a feladatra megbízott alkalmazott érhesse el.

42. § Ha a papír alapú, személyes adatokat tartalmazó munkadokumentumok használata már nem szükséges, olyan módon kell azokat megsemmisíteni (pl.: irat ledarálásával), hogy a megsemmisítést követően ne lehessen azok tartalmát megállapítani.

43. § Tilos magánhasználatú eszközön az Adatkezelő kezelésében, vagy feldolgozásában lévő személyes adatot tárolni, kivéve, ha a tárolás a munkavégzéshez elengedhetetlenül szükséges és a tárolást a munkavégzést követően megszüntetik.

44. § Az alkalmazott feladatellátásra szolgáló jogviszonya megszűnése esetén minden személyes adatot is tartalmazó papír alapú és elektronikus iratot, adatot köteles a foglalkoztatásának utolsó napját megelőzően az Adatkezelő részére visszaszolgáltatni, azokról másolatot nem tarthat magánál, melyről átadás-átvételi jegyzőkönyvet kell készíteni.

45. § Minden alkalmazott köteles az általa használt munkaterületet olyan módon használni, hogy azon az Adatkezelő kezelésében, vagy feldolgozásában lévő, személyes adatot is tartalmazó dokumentumok lehetőség szerint szabadon ne legyenek hozzáférhetők. Ilyen intézkedésnek minősül különösen: számítástechnikai eszközök jelszavas védelme, az irodahelyiség zárása, az iratok elhelyezése védett helyre. Adatkezelő minden munkatársa köteles biztosítani és megfelelő intézkedéseket megtenni annak érdekében, hogy az Adatkezelő valamennyi irodai területére az Adatkezelővel feladatvégzésre irányuló jogviszonyban nem álló személy csak alkalmazott kíséretében léphessen be. Az Adatkezelő területére belépni jogosult személyek az Adatkezelő által kezelt személyes adatok megismerésére nem minden esetben jogosultak. Az alkalmazottak kötelesek megtenni mindent annak érdekében, hogy az Adatkezelő kezelésében álló személyes

adatok biztonságban legyenek, az ennek megsértéséből az Adatkezelőt ért kárért az adatvédelmi incidenst előidéző személy teljes felelősséggel tartozik.

46. § Személyes adatok csak biztonságos kommunikációs csatorna alkalmazásával, illetve megfelelő titkosítási megoldással adhatók át más személynek. Ellenkező jelzésig az Adatkezelő belső levelezési rendszerén belüli adatáramlás biztonságos kézbesítési csatornának tekintendő. Külső adatátadás során gondoskodni kell a személyes adatok titkosításáról SSL-kapcsolat, vagy egyedi titkosítás használatával, a jelszó elkülönített csatornán (pl.: SMS) keresztüli küldésével, papír alapon pedig zárt borítékon keresztüli átadással.

47. § Amennyiben az Adatkezelő más adatkezelőtől, az adathoz kapcsolódó rendelkezéssel fogad személyes adatot, valamennyi, az adattal érintkező felhasználónak kötelessége az adattovábbító rendelkezéseit figyelembe venni.

48. § Harmadik személynek titoktartási nyilatkozat hiányában személyes adat nem adható ki.

VII. Adatvédelmi incidensekkel kapcsolatos kötelezettségek

49. § Adatvédelmi incidens alatt a Rendelet értelmében a biztonság olyan sérülését értjük, amely

- a továbbított,
- tárolt vagy
- más módon kezelt

személyes adatok véletlen vagy jogellenes

- megsemmisítését,
- elvesztését,
- megváltoztatását,
- jogosulatlan közlését vagy
- az azokhoz való jogosulatlan hozzáférést

eredményezi.

50. § Az adatvédelmi incidens megfelelő és kellő idejű intézkedés hiányában fizikai, vagyoni vagy nem vagyoni károkat okozhat a természetes személyeknek, többek között a személyes adataik feletti rendelkezés elvesztését vagy a jogaik korlátozását, a hátrányos megkülönböztetést, a személyazonosság-lopást vagy a személyazonossággal való visszaélést, a pénzügyi veszteséget, az álnevesítés engedély nélküli feloldását, a jó hírnév sérelmét, a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülését, illetve a szóban forgó természetes személyeket sújtó egyéb jelentős gazdasági vagy szociális hátrányt. Ezért a jelen szabályzat hatálya alá tartozó személyek, bármely, az Adatkezelő által vagy közreműködésével működtetett informatikai rendszer vagy manuális adatkezelés esetében haladéktalanul, de legkésőbb 24 órán belül kötelesek jelenteni az adatvédelmi tisztviselő számára, ha adatvédelmi incidens gyanúja merül fel, vagy ha biztos tudomása van arról, hogy adatvédelmi incidens történt.

A bejelentést elsősorban munkaidőben, telefonon keresztül kell megtenni, és azt követően az adatvédelemért felelős személy számára küldött elektronikus levél formájában is meg kell erősíteni.

51. § Az adatvédelmi tisztviselő és az egyéb érintett személyek a számukra jelzett, vagy saját feladat- vagy hatáskörükben megállapított adatvédelmi incidens felderítése és súlyosságának megállapítása érdekében a jelen §-ban foglalt eljárásrend szerint kötelesek eljárni:

a) Adatkezelő minden szükséges intézkedést megtesz az adatvédelmi incidensek elkerülése érdekében.

b) Amennyiben mégis adatvédelmi incidens következik be az adatvédelmi tisztviselő felveszi a kapcsolatot az adatvédelmi incidenssel érintett informatikai rendszer rendszergazdájával, az adatvédelmi incidenssel érintett adatkezelési folyamat adatgazdájával, és ha azonosítható ilyen, az incidenst előidéző személlyel.

c) Az adatvédelmi tisztviselő a felderítés során az alábbi kategóriák valamelyikébe kell az adatvédelmi incidenst sorolni:

1. Alacsony szintű adatvédelmi incidens: a személyes adatok elhanyagolható körének jogosulatlan továbbítása, megváltoztatása, nyilvánosságra hozatala, szándékolt, vagy véletlen törlése vagy megsemmisítése, vagy más jogellenes adatkezelési eset.

2. Közepes szintű adatvédelmi incidens: a személyes adatok csekély körének megváltoztatása, jogosulatlan továbbítása, nyilvánosságra hozatala, szándékolt, vagy véletlen törlése vagy megsemmisítése, vagy más jogellenes adatkezelési eset.

3. Magas szintű adatvédelmi incidens: a személyes adatok széles körének jogosulatlan megváltoztatása, továbbítása, nyilvánosságra hozatala, szándékolt, vagy véletlen törlése vagy megsemmisítése, vagy más jogellenes adatkezelési eset, illetve az adatok körétől függetlenül minden olyan eset, amikor valószínűsíthető, hogy az incidensnek az érintettre hátrányos hatása van, vagy biztosra vehető, hogy az incidensnek az érintettre hátrányos hatása van.

d) Intézkedések:

1. Alacsony szintű adatvédelmi incidens esetén az adatvédelmi tisztviselő:

1.1. legkésőbb a tudomásszerzéstől számított 2 napon belül az érintett rendszer rendszergazdájával és az adatvédelmi incidenssel érintett adatkezelési folyamat adatgazdájával meghatározza az adatvédelmi incidens kezelésének módját és felhívja az intézkedésre jogosult személyt az incidens kezelésére,

1.2. rögzíti az adatvédelmi incidenst az incidensek nyilvántartásába.

2. Közepes szintű adatvédelmi incidens esetén az adatvédelmi tisztviselő:

2.1. haladéktalanul, de legkésőbb a tudomásszerzéstől számított 24 órán belül munkacsoportot hív össze, amelyben részt vesz az adatvédelemért felelős

személyen kívül a rendszergazda, az adatvédelmi incidenssel érintett adatkezelési folyamat adatgazdája és Adatkezelő vezetője,

2.2. az adatvédelmi tisztviselő rögzíti az adatvédelmi incidenst az incidensek nyilvántartásában,

2.3. az adatvédelmi tisztviselő értesíti a felügyeleti hatóságot 72 órán belül

2.4. adatvédelmi incidensről, ha az adatvédelmi incidens valószínűsíthetően kockázattal jár az érintett vagy más érintettek jogaira és szabadságaira nézve és a munkacsoport meghatározza az adatvédelmi incidens kezelésének módját és felhívja az intézkedésre jogosult személyt az incidens kezelésére.

3. Magas szintű adatvédelmi incidens esetén

3.1. az adatvédelmi tisztviselő haladéktalanul, de legkésőbb a tudomásszerzéstől számított 24 órán belül munkacsoportot hív össze, amelyben részt vesz az adatvédelmi tisztviselő kívül a rendszergazda, az adatvédelmi incidenssel érintett adatkezelési folyamat adatgazdája és Adatkezelő vezetője,

3.2. a munkacsoport meghatározza az adatvédelmi incidens kezelésének módját és felhívja az intézkedésre jogosult személyt az incidens kezelésére, továbbá meghatározza az érintettek értesítésének módját, az értesítés tartalmát, és gondoskodik az érintettek haladéktalan értesítéséről,

3.3. az adatvédelmi tisztviselő rögzíti az adatvédelmi incidenst az incidensek nyilvántartásában,

3.4. az adatvédelmi tisztviselő értesíti a felügyeleti hatóságot a tudomásszerzéstől számított 72 órán belül az adatvédelmi incidensről.

e) Az Adatkezelő az adatvédelmi tisztviselő útján az adatvédelmi incidenssel kapcsolatos intézkedések ellenőrzése, valamint az érintett tájékoztatása céljából az adatvédelmi incidensekről nyilvántartást vezet, amely tartalmazza az adatvédelmi incidenssel érintett személyes adatok körét, az adatvédelmi incidenssel érintettek körét és számát, az adatvédelmi incidens időpontját, körülményeit, hatásait és az elhárítására megtett intézkedéseket, valamint az adatkezelést előíró jogszabályban meghatározott egyéb adatokat.

f) Amennyiben az érintett ezt kéri, az az adatvédelmi tisztviselő tájékoztatást ad az érintett személyes adatára is kiterjedő adatvédelmi incidensekkel kapcsolatban. Adatkezelő nem köteles tájékoztatni az érintettet az adatvédelmi incidensről, ha

1. Adatkezelő megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre, és ezeket az intézkedéseket az adatvédelmi incidens által érintett adatok tekintetében alkalmazta (különösen azokat az intézkedéseket – mint például a

titkosítás alkalmazása –, amelyek a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik az adatokat).

2. Adatkezelő az adatvédelmi incidenst követően olyan további intézkedéseket tett, amelyek biztosítják, hogy az érintett jogaira és szabadságaira jelentett magas kockázat a továbbiakban valószínűsíthetően nem valósul meg.

3. A tájékoztatás aránytalan erőfeszítést tenne szükségessé az Adatkezelő részéről. Ilyen esetekben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, vagy olyan hasonló intézkedést kell hozni, amely biztosítja az érintettek hasonlóan hatékony tájékoztatását. Pl. sajtóközlemény kiadása.

Ha Adatkezelő nem értesítette az érintettet az adatvédelmi incidensről, az incidens bejelentését követően a felügyeleti hatóság, miután mérlegelte, hogy az adatvédelmi incidens valószínűsíthetően magas kockázattal jár-e, elrendelheti az érintett tájékoztatását, vagy megállapíthatja, hogy az érintett tájékoztatása az e §-ban foglalt valamely ok miatt nem szükséges.

g) Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az Adatkezelő indokolatlan késedelem nélkül köteles írásban, vagy ha rendelkezésre áll email cím, akkor e-mailben tájékoztatni az érintettet az adatvédelmi incidensről. A tájékoztatásban világosan és közérthetően ismertetni kell az adatvédelmi incidens jellegét, és közölni kell legalább az alábbi információkat:

1. az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;

2. ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket;

3. ismertetni kell az Adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

52. § Adatvédelmi incidens nem csak Adatkezelőnél merülhet fel, hanem a vele szerződéses kapcsolatban álló adatfeldolgozónál is.

a) Ha az adatfeldolgozó rendszerében észlel adatvédelmi incidenst, indokolatlan késedelem nélkül köteles bejelenteni azt Adatkezelőnek, illetve amennyiben nem lehetséges az információkat egyidejűleg közölni, azokat köteles további indokolatlan késedelem nélkül akár részletekben is közölni.

b) Amennyiben Adatkezelő észlel adatvédelmi incidenst valamely adatfeldolgozójánál, vagy adatvédelmi incidens gyanúja merül fel, akkor Adatkezelő az Adatfeldolgozó egyidejű értesítésével lefolytatja az adatvédelmi incidens azonosításával és kezelésével kapcsolatos, jelen pont szerinti eljárását.

c) Az Adatfeldolgozó az – Adatfeldolgozási szerződésben foglal kötelezettsége szerinti – az Adatkezelővel egyeztetve köteles az incidens kezelésében együttműködni, illetve köteles minden olyan megfelelő technikai és szervezési intézkedéseket végrehajtani, ami a hasonló, vagy ugyanolyan adatvédelmi incidens elkerülése érdekében szükséges, és az incidens ismételt bekövetkezésének lehetőségét kizárja.

d) Az adatvédelmi incidens bejelentésének elmaradásából, az incidens nem megfelelő kezeléséből és az együttműködési kötelezettség megszegéséből fakadó felelősség az Adatfeldolgozót terheli.

VIII. Új adatkezelési tevékenység

53. § Személyes adatok kezelésével járó új tevékenységek bevezetésekor az alábbi feladatokat kell elvégeznie az adatvédelemért felelős személynek:

a) meg kell határoznia

1. a kezelendő személyes adatok körét,
2. az adatok kezelésének célját,
3. az adatkezelés jogalapját,
4. az adatkezelés időtartamát,

b) fel kell mérnie, hogy az adatok milyen informatikai rendszerben lesznek kezelve, az adatok milyen informatikai rendszerben jelennek meg,

c) meg kell határoznia, hogy előreláthatóan az adatokhoz kinek szükséges hozzáférnie az Adatkezelő-en belül, illetve kívül,

d) be kell mutatni, hogy az adatokat szükséges-e továbbítani más személy számára,

e) be kell mutatni, hogy az adatkezeléshez igénybe kell-e venni adatfeldolgozót, amennyiben igen, az adatfeldolgozó feladata mi lesz, várhatóan ki lesz az adatfeldolgozó,

f) meg kell határozni az adatkezelés megkezdésének tervezett időpontját, az adatok felvételének módját és pontos helyét (pl.: erre szolgáló internetes felület vagy papír alapú adatfelvétel).

54. § A kialakított adatkezelési terv alapján az adatkezelésről szóló tájékoztatót és a végleges adatfeldolgozási szerződést az adatvédelmi tisztviselő készíti el.

I. Közérdekű adatok nyilvánossága

55.§ A közérdekű adatokat a hivatal (a személyes és a minősített, illetve az Infotv. vagy egyéb törvény által ás okból korlátozott megismerhetőségű adatok kivételével) a www.fulopszallas.hu honlapon rendszeresen közzéteszi.

56.§ A hivatal által bármilyen formában nyilvánosságra hozott dokumentumot lehetőség szerint elektronikus úton is közre kell bocsátani.

57.§ Az egyes hatósági és más konkrét ügyek intézésére, a jogszabályi előírásokra, illetve egyéb közérdekű adatokra vonatkozó szóbeli vagy írásbeli információkérésnek feladatkörén belül – sajtó esetében a jegyző előzetes tájékoztatása és egyetértése mellett – minden köztisztviselő köteles pontosan és haladéktalanul eleget tenni. Jelen fejezetben szabályozottak végrehajtására Fülöpszállás Község Polgármesteri Hivatalának a közérdekű adatok megismerésére irányuló igények teljesítésének rendjéről szóló szabályzata az irányadó.

II. Fülöpszállás Polgármesteri Hivatal Anyakönyvi Szolgáltató Alrendszer (ASZA) használatára vonatkozó rendelkezések

58.§ A biztonsági okmányok védelmének rendjéről szóló 86/1996. (VI. 14.) Korm. rendelet 1. sz. melléklete alapján az anyakönyvi kivonat és anyakönyv biztonsági okmány. Az okmánykezelésről az anyakönyvekről, a házasságkötési eljárásról és a névviselésről szóló 6/2003. (III. 7.) BM rendelet 6. sz. melléklete rendelkezik.

59.§ Az ASZA rendszert hozzáférési jogosultsággal rendelkező anyakönyvvezető használhatja. Az ASZA rendszer használatához szükséges hozzáférési jogosultságok és a felhasználói kártyák igényléséről és kezeléséről a 6/2003. (III. 7.) BM rendelet 7. sz. melléklete rendelkezik.

60.§ A jegyző a helyi jogosultságokról nyilvántartást vezet.

III. Záró rendelkezések

61.§ Amennyiben a bíróság, a Nemzeti Adatvédelmi és Információszabadság Hatóság az Adatkezelőt személyes adatok jogsértő kezelési miatt elmarasztalja vagy kártérítésre kötelezi, az az érintett köztisztviselő anyagi, fegyelmi, illetve büntetőjogi felelősségre vonását alapozza meg.

62.§ A közszolgálati tisztviselőkről szóló 2011. évi CXCIX. törvény 177.§ (4) bekezdésében kapott felhatalmazás alapján külön Közszolgálati adatvédelmi szabályzatban határozom meg a közszolgálati iratok, adatok kezelésének adatvédelmi, adatbiztonsági szabályait.

63.§ Jelen szabályzat 2018. augusztus 1. napján lép hatályba. A szabályzat hatálybalépésével egyidejűleg hatályát veszti Fülöpszállás Polgármesteri Hivatalának Adatvédelmi és Adatbiztonsági Szabályzata. A szabályzat módosítása esetén az Adatkezelő a belső szabályzatokra irányadó módon hirdeti ki a módosított szabályzatot.

Fülöpszállás, 2018.július 18.

Simon László István

jegyzői feladatokat ellátó aljegyző

1. melléklet

Adatvédelmi incidensek nyilvántartása

Az adatvédelmi incidens időpontja	Az adatvédelmi incidenssel érintettek köre és száma	Érintett személyes adatok körének megjelölése	Az adatvédelmi incidens körülményei, hatásai	Az adatvédelmi incidens hatásai	Az elhárítására megtett intézkedések