

**SAJÓSZENTPÉTER VÁROSI
ÖNKORMÁNYZAT
SAJÓSZENTPÉTERI POLGÁRMESTERI
HIVATAL**

6/2018.

**ADATVÉDELMI ÉS ADATBIZTONSÁGI
SZABÁLYZATA**

Hatályos: 2018. május 15. napjától



TARTALOMJEGYZÉK

I.	ÁLTALÁNOS RENDELKEZÉSEK.....	4
1.	A szabályzat célja.....	4
2.	A szabályzat hatálya.....	4
3.	Értelmező rendelkezések.....	4
II.	AZ ADATVÉDELEM SZERVEZETE	7
1.	A jegyző	7
2.	A belső adatvédelmi felelős (adatvédelmi tisztviselő).....	7
3.	Osztályvezetők	8
4.	A rendszergazda	8
5.	Az adatkezelő	8
III.	A SZEMÉLYES ADATOK KEZELÉSE ÉS TOVÁBBÍTÁSA.....	9
1.	ADATKEZELÉS, ADATBIZTONSÁG.....	9
2.	AZ ADATSZOLGÁLTATÁS RENDJE.....	11
3.	KÖZÉRDEKŰ ADATOK NYILVÁNOSSÁGA.....	13
IV.	A KÉPVISELŐ-TESTÜLETI ÜLÉSEKKEL, BIZOTTSÁGI ÜLÉSEKKEL KAPCSOLATOS IRATANYAG KEZELÉSÉRE VONATKOZÓ KÜLÖN SZABÁLYOK.....	13
V.	AZ INFORMÁCIÓBIZTONSÁG VONATKOZÁSAI AZ ADATVÉDELEMBEN ÉS ADATBIZTONSÁGBAN.....	14
VI.	ZÁRÓ RENDELKEZÉSEK.....	18

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 2 / 18



Verzió	Készült/módosult	Változás oka	Jóváhagyta	Hatálybalépés dátuma
1.0	2018.05.04.	Első verzió		
1.1	2018.08.15.	GDPR pontosítások		



Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény 24. § (3) bekezdésében és 30. § (6) bekezdésében kapott felhatalmazás alapján Sajószentpéter Városi Önkormányzat, valamint a Sajószentpéteri Polgármesteri Hivatal adatvédelmi és adatbiztonsági szabályait az alábbiak szerint határozzuk meg:

I. fejezet

Általános rendelkezések

1. A szabályzat célja

- 1.1. A szabályzat célja Sajószentpéter Városi Önkormányzat (a továbbiakban: Önkormányzat) és a Sajószentpéteri Polgármesteri Hivatal (a továbbiakban: Hivatal) által végzett adatkezelések, adatfeldolgozások során a személyes adatok védelme és a közérdekű és közérdekből nyilvános adatok hozzáférhetőségének biztosítása.
- 1.2. A személyes adatok védelméhez fűződő jogot és az érintett személyiségi jogait, ha törvény kivételt nem tesz, az adatkezeléshez fűződő más érdekek – ideértve a közérdekű adatok nyilvánosságát is – nem sérthetik.
- 1.3. Az adatvédelmet
 - az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.), valamint
 - az Európai Parlament és a Tanács (EU) 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 2016/679 rendelete (általános adatvédelmi rendelet, a továbbiakban: GDPR) rendelkezéseivel összhangban kell alkalmazni.

2. A szabályzat hatálya

- 2.1. A szabályzat tárgyi hatálya - figyelemmel az Infotv. 2. §-ában foglaltakra - kiterjed az Önkormányzat és a Hivatal által folytatott minden olyan adatkezelésre, amely személyes adatra, valamint közérdekű adatra vagy közérdekből nyilvános adatra vonatkozik.
- 2.2. A szabályzat személyi hatálya kiterjed az Önkormányzatnál és a Hivatalban foglalkoztatott valamennyi köztisztviselőre, ügykezelőre, munkaviszony keretében, továbbá megbízási szerződéssel foglalkoztatottakra (a továbbiakban: munkavállalók).

3. Értelmező rendelkezések

3.1. személyes adat: azonosított vagy azonosítható természetes személyre („érintett”) vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható;

3.2. különleges adat: a személyes adatok különleges kategóriába tartozó minden adat, azaz a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a genetikai adatok, a természetes személyek egyedi azonosítását célzó biometrikus adatok, az egészségügyi adatok és a

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 4 / 18



természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok;

3.3. közérdekű adat: az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő és tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől, így különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre, annak eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat;

3.4. közérdekből nyilvános adat: a közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli.

3.5. adatkezelés: a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés;

3.6. az adatkezelés korlátozása: a tárolt személyes adatok megjelölése jövőbeli kezelésük korlátozása céljából;

3.7. profilalkotás: személyes adatok automatizált kezelésének bármely olyan formája, amelynek során a személyes adatokat valamely természetes személyhez fűződő bizonyos személyes jellemzők értékelésére, különösen a munkahelyi teljesítményhez, gazdasági helyzetéhez, egészségi állapothoz, személyes preferenciákhoz, érdeklődéshez, megbízhatósághoz, viselkedéshez, tartózkodási helyhez vagy mozgáshoz kapcsolódó jellemzők elemzésére vagy előrejelzésére használják;

3.8. álnevesítés: személyes adat olyan módon történő kezelése, amely – a személyes adattól elkülönítve tárolt – további információ felhasználása nélkül megállapíthatatlanná teszi, hogy a személyes adat mely érintettre vonatkozik, valamint műszaki és szervezési intézkedések megtételével biztosítja, hogy azt azonosított vagy azonosítható természetes személyhez ne lehessen kapcsolni;

3.9. nyilvántartási rendszer: a személyes adatok bármely módon – centralizált, decentralizált vagy funkcionális vagy földrajzi szempontok szerint – tagolt állománya, amely meghatározott ismérvek alapján hozzáférhető;

3.10. adatkezelő: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely – törvényben vagy az Európai Unió kötelező jogi aktusában meghatározott keretek között – önállóan vagy másokkal együtt az adat kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja;

3.11. adatfeldolgozó: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely - törvényben vagy az Európai Unió kötelező jogi aktusában meghatározott keretek között és feltételekkel – az adatkezelő megbízásából vagy rendelkezése alapján személyes adatokat kezel;

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 5 / 18



3.12. címzett: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely részére személyes adatot az adatkezelő, illetve az adatfeldolgozó hozzáférhetővé tesz;

3.13. harmadik személy: olyan természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely nem azonos az érintettel, az adatkezelővel, az adatfeldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére irányuló műveleteket végeznek;

3.14. hozzájárulás: az érintett akaratának önkéntes, határozott és megfelelő tájékoztatáson alapuló egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy az akaratát félreérthetetlenül kifejező más magatartás útján jelzi, hogy beleegyezését adja a rá vonatkozó személyes adatok kezeléséhez;

3.15. adatvédelmi incidens: az adatbiztonság olyan sérelme, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisülését, elvesztését, módosulását, jogosulatlan továbbítását vagy nyilvánosságra hozatalát, vagy az azokhoz való jogosulatlan hozzáférést eredményezi;

3.16. genetikai adat: egy természetes személy örökölt vagy szerzett genetikai jellemzőire vonatkozó minden olyan személyes adat, amely az adott személy fiziológiájára vagy egészségi állapotára vonatkozó egyedi információt hordoz, és amely elsősorban az említett természetes személyből vett biológiai minta elemzéséből ered;

3.17. biometrikus adat: egy természetes személy testi, fiziológiai vagy viselkedési jellemzőire vonatkozó minden olyan sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását, ilyen például az arckép vagy a daktiloszkópiai adat;

3.18. egészségügyi adat: egy természetes személy testi vagy pszichikai egészségi állapotára vonatkozó személyes adat, ideértve a természetes személy számára nyújtott egészségügyi szolgáltatásokra vonatkozó olyan adatot is, amely információt hordoz a természetes személy egészségi állapotáról;

3.19. felügyeleti hatóság: Magyarországon a jogkört a Nemzeti Adatvédelmi és Információszabadság Hatóság tölti be, feladata a személyes adatok védelméhez, valamint a közérdekű és a közérdekből nyilvános adatok megismeréséhez való jog érvényesülésének ellenőrzése és elősegítése, továbbá a személyes adatok Európai Unión belüli szabad áramlásának elősegítése;

3.20. érintett felügyeleti hatóság: az a felügyeleti hatóság, amelyet a személyes adatok kezelése a következő okok valamelyike alapján érint: a) az adatkezelő vagy az adatfeldolgozó az említett felügyeleti hatóság tagállamának területén rendelkezik tevékenységi hellyel; b) az adatkezelés jelentős mértékben érinti vagy valószínűsíthetően jelentős mértékben érinti a felügyeleti hatóság tagállamában lakóhellyel rendelkező érintetteket; vagy c) panaszt nyújtottak be az említett felügyeleti hatósághoz;

3.21. nemzetközi szervezet: a nemzetközi közjog hatálya alá tartozó szervezet vagy annak alárendelt szervei, vagy olyan egyéb szerv, amelyet két vagy több ország közötti megállapodás hozott létre vagy amely ilyen megállapodás alapján jött létre.

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 6 / 18



II. fejezet

Az adatvédelem szervezete

1. A jegyző:

Ellátja a törvény által a hatáskörébe utalt feladatokat, ennek keretében:

- 1.1. A polgármesterrel közösen kiadja az adatvédelmi és adatbiztonsági szabályzatot.
- 1.2. Kinevezi (megbízta) a Hivatal belső adatvédelmi felelősét (adatvédelmi tisztviselőjét).
- 1.3. Dönt a szervezeten kívüli adatfeldolgozók személyéről vagy szervezetről és az adatfeldolgozásra vonatkozó szerződésről.
- 1.4. Meghatározza az osztályvezetők javaslata alapján, a szervezeten kívüli személy vagy szervezet által elvégzendő adatkarbantartások időpontjait.
- 1.5. Ellenőrzi az adatkezelést és adatvédelmet, valamint az informatikát érintő nyilvántartásokat a belső ellenőr, az osztályvezetők, valamint a belső adatvédelmi felelős (adatvédelmi tisztviselő) útján.

2. A belső adatvédelmi felelős (adatvédelmi tisztviselő)

- 2.1. Közreműködik, illetve segítséget nyújt az adatkezeléssel összefüggő döntések meghozatalában, valamint az érintettek jogainak biztosításában.
- 2.2. Ellenőrzi az adatkezelésre vonatkozó jogszabályok, valamint a belső adatvédelmi és adatbiztonsági szabályzatok rendelkezéseinek és az adatbiztonsági követelményeknek a megtartását.
- 2.3. Kivizsgálja a hozzá érkezett bejelentéseket, jogosulatlan adatkezelés észlelése esetén annak megszüntetésére szólítja fel az adatkezelőt vagy az adatfeldolgozót.
- 2.4. Elkészíti és folyamatosan aktualizálja a belső adatvédelmi és adatbiztonsági szabályzatot.
- 2.5. Gondoskodik az adatvédelmi ismeretek oktatásáról.
- 2.6. Felkérés alapján véleményezi - adatvédelmi szempontból - a képviselő-testületi és a bizottsági előterjesztéseket.
- 2.7. Megkeresésre véleményezi az adatszolgáltatás iránti kérelmeket.
- 2.8. Összesíti a polgármesteri hivatal adatkezelői által közérdekű adatok iránti kérelmek elutasításáról, valamint az elutasítások indokairól vezetett nyilvántartást, majd az abban foglaltakról minden évben január 31-éig tájékoztatja a Nemzeti Adatvédelmi és Információszabadság Hatóságot.
- 2.9. Tájékoztat és szakmai tanácsot ad az adatkezelést végző munkavállalók részére az adatvédelmi rendelkezések szerinti kötelezettségeikkel kapcsolatban.
- 2.10. Kérésre szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, valamint nyomon követi a hatásvizsgálat elvégzését.
- 2.11. Együttműködik a felügyeleti hatósággal.
- 2.12. Az adatkezeléssel összefüggő ügyekben kapcsolattartó pontként szolgál a felügyeleti hatóság felé, valamint adott esetben bármely egyéb kérdésben konzultációt folytat vele.
- 2.13. Ellátja a jegyző által esetenként meghatározott adatvédelmi feladatokat.

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 7 / 18



3. Osztályvezetők

- 3.1. Ellenőrzik az adat- és az adatszolgáltatási nyilvántartás naprakészességét.
- 3.2. Meghatározzák az irányításuk alatt álló szervezeti egység adatkezelőinek hozzáférési jogosultságait.
- 3.3. Koordinálják az adott osztályon dolgozó adatkezelők tevékenységét.
- 3.4. Gondoskodnak az adatkezelők helyettesítési rendjéről.
- 3.5. Javaslatot tesznek a jegyzőnek a szervezeten kívüli adatfeldolgozók személyére vagy szervezetre, az általuk elvégzendő adatkarbantartások időpontjára.
- 3.6. Biztosítják az irányításuk alá tartozó szervezeti egységnél az adatkezelés és az adatvédelem rendjét.

4. A rendszergazda

A rendszergazda a jegyző és az osztályvezető vezetése alatt:

- 4.1. A szervereken tárolt adatok vonatkozásában gondoskodik a kezelt adatokhoz való jogosulatlan hozzáférés, módosítás megakadályozásáról, illetőleg gondoskodik a tárolt adatok megsemmisülésének megakadályozásáról.
- 4.2. Igény esetén közreműködik a számítógépen/szerveren tárolt adatok esetében a megadott szempontú adatszolgáltatásban.
- 4.3. Elvégzi a szervereken tárolt adatok biztonsági mentését, naplózását.
- 4.4. Ellátja a polgármester, a jegyző, valamint az osztályvezetők által az adatkezeléssel kapcsolatos esetenként meghatározott feladatokat.
- 4.5. Igény esetén segítséget nyújt az adatkezelőknek a számítástechnikai alkalmazások használatánál és az adatbázisok kezelésénél.

5. Az adatkezelő

- 5.1. Kezeli a munkakörébe tartozó adatokat, más adatot csak helyettesítés esetén kezelhet, vezeti a nyilvántartásokat.
- 5.2. A jogszabály által felhatalmazott személynek vagy szervezetnek adatot szolgáltat.
- 5.3. Vezeti az adat-, valamint az adatszolgáltatási nyilvántartást.
- 5.4. Megőrzi a tudomására jutott adatot.
- 5.5. Gondoskodik arról, hogy az általa vezetett nyilvántartás adataihoz illetéktelen személy ne férhessen hozzá, ügyel a nyilvántartás biztonságos tárolására.
- 5.6. Betartja az adatkezelésre, adatvédelemre és az adatbiztonságra vonatkozó rendelkezéseket.
- 5.7. Haladéktalanul jelzi az osztályvezetőnek a számítástechnikai eszközök bármilyen meghibásodását, illetőleg az adatállomány kezelhetőségében bekövetkező problémát.
- 5.8. Az adatkezelő köteles a közvetlen vezetőjét és a belső adatvédelmi felelőst (adatvédelmi tisztviselőt) tájékoztatni minden olyan eseményről, mely esetben őt jogszerűtlen adatkezelésre kérték fel, utasították, illetve a saját rendszerében bármilyen egyéb illetéktelen adathozzáférést, vagy adatkezelést tapasztalt.

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 8 / 18



III. fejezet A személyes adatok kezelése és továbbítása

1. Adatkezelés, adatbiztonság

1.1. Személyes adat kizárólag egyértelműen meghatározott, jogszerű célból, jog gyakorlása és kötelezettség teljesítése érdekében kezelhető. Az adatkezelésnek minden szakaszában meg kell felelnie az adatkezelés céljának, az adatok gyűjtésének és kezelésének tisztességének és törvényesnek kell lennie.

1.2. Személyes adat akkor kezelhető, ha:

- a) azt törvény vagy – törvény felhatalmazása alapján, az abban meghatározott körben, különleges adatnak vagy bűnügyi személyes adatnak nem minősülő adat esetén – helyi önkormányzat rendelete közérdeken alapuló célból elrendeli,
- b) az a) pontban meghatározottak hiányában az az adatkezelő törvényben meghatározott feladatainak ellátásához feltétlenül szükséges és az érintett a személyes adatok kezeléséhez kifejezetten hozzájárult,
- c) az a) pontban meghatározottak hiányában az az érintett vagy más személy létfontosságú érdekeinek védelméhez, valamint a személyek életét, testi épségét vagy javait fenyegető közvetlen veszély elhárításához vagy megelőzéséhez szükséges és azzal arányos, vagy
- d) az a) pontban meghatározottak hiányában a személyes adatot az érintett kifejezetten nyilvánosságra hozta és az az adatkezelés céljának megvalósulásához szükséges és azzal arányos.

1.3. Különleges adatok kezelésével járó ügyekben a jelen szabályzatban foglaltakon túl is megkülönböztetett gondossággal kell eljárni. Figyelemmel kell lenni arra, hogy különleges adatok kizárólag törvényi felhatalmazás alapján, illetve az érintett írásbeli hozzájárulásával kezelhetők.

1.4. A személyes adatok célhoz kötöttségének elve alapján, az egyes eljárások során kezelt adatokat csak az adott ügy elintézése érdekében szabad felhasználni, más eljárásokkal, illetve adatokkal nem kapcsolhatók össze, kivéve, ha törvény megengedi, illetve az érintett hozzájárult és az adatkezelés feltételei minden egyes személyes adatra vonatkozóan fennállnak. Konkrét ügyben hivatalból csak azokat a személyes adatokat lehet rögzíteni, amelyek kezelésére törvény, vagy törvény felhatalmazása alapján önkormányzati rendelet, illetve az érintett felhatalmazást ad, mellőzve a bemutatott személyazonosító és egyéb okmányok, személyes iratok indokolatlan fénymásolását és megőrzését.

1.5. 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.

1.6. 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.

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 9 / 18



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.

1.7. Az adattörlés maradéktalan megvalósítása érdekében az irattározásra kerülő anyagok selejtezési idejét, irattári jelét a hivatal Iratkezelési Szabályzatának mellékletét képező Irattári Terv határozza meg.

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

1.9. Személyes adatokat tartalmazó iratok telefaxon, elektronikus úton, illetve az abban foglalt adatok telefonon csak kellő körültekintéssel továbbíthatók.

1.10. A munkavállalónál, illetve irattárban lévő iratba az ügyintéző hivatali köztisztviselőn kívül más személy – a vonatkozó eljárásjogi szabályok szerint – csak akkor tekinthet be, ha ezt jogszabály lehetővé teszi, illetve az illetékes vezető ezt engedélyezte. A betekintési jog gyakorlása során úgy kell eljárni, hogy ez által mások személyes adatainak védelméhez fűződő jogai, illetve személyiségi jogai ne sérülhessenek. E rendelkezést kell alkalmazni a másolat, kivonat készítésekor is.

1.11. A munkavállaló 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 munkavállalónál.

1.12. A képviselő-testületi és a bizottsági ülésekről, valamint a nemzetiségi önkormányzatok üléseiről készült jegyzőkönyvek közül a zárt ülések jegyzőkönyveit fokozott gondossággal kell kezelni. A zárt ülések jegyzőkönyveit külön kell lefűzni vagy bekötetni, zárható szekrényben kell tárolni. További szabályokat ide vonatkozóan a IV. fejezet tartalmaz.

1.13. Az ügyfélfogadáshoz a köztisztviselők részére lehetőség szerint külön szobát kell biztosítani.

1.14. A munkavállalók irodai helyiségüket és az irat és adattárolásra használt berendezéseket munkaidőben fokozott gondossággal kötelesek őrizni. A munkavállaló 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.

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 10 / 18



- 1.15. A tűz elleni védekezés rendjét és elhárítása érdekében szükséges intézkedéseket a Tűzvédelmi Szabályzat tartalmazza.
- 1.16. Az egyes nyilvántartások, adatkezelések tekintetében a hozzáférési jogosultságot az illetékes szervezeti egység vezetőjének személyre szólóan meg kell határozni és az időszerű állapotnak megfelelően a rendszergazdának nyilván kell tartania. Az adatok nyilvántartása történhet elektronikus, illetve manuális módon. Nem tárolható lényeges adatállomány a számítógépek saját tárolóin, azok tárolása kizárólag a hálózaton történik.
- 1.17. A személyes adatok akkor továbbíthatóak, valamint a különböző adatkezelések akkor kapcsolhatóak 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.
- 1.18. 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 értesítendőök jegyzékét, arról tájékoztatást adni azonban csak a vonatkozó jogszabályok és jelen szabályzat rendelkezéseinek figyelembevételével lehet.
- 1.19. A Hivatalban a számítógépek és a levelező rendszer kizárólag munkavégzés céljából használhatóak, azon magánjellegű adatokat tárolni nem szabad.
- 1.20. Az álláspályázati eljárásokkal kapcsolatos adatokat a pályázati eljárás lezárásáig szabad őrizni. A pályázók az eredménytelen pályázatok részükre történő visszaküldésével egyidejűleg értesítésre kerülnek adataik törléséről.
- 1.21. A munkavállalók személyi anyagait a közszolgálati tisztviselőkről szóló 2011. évi CXCV. törvény 184. § (4) bekezdése alapján a jogviszony megszűnésétől számított 50 évig meg kell őrizni.

2. Az adatszolgáltatás rendje

- 2.1. Az érintettet a törvény szerint megilleti az a jog, hogy személyes adatai kezeléséről tájékoztatást kérjen, továbbá kérheti adatainak helyesbítését, az adatkezelés korlátozását vagy az adatok törlését (Infotv. 14. §). A jelen pont szerinti tartalmú kérelmeket (a jogszabályi feltételek fennállása esetén) azok benyújtásától számított legrövidebb idő alatt, de legfeljebb huszonöt napon belül el kell bírálni és a döntésről az érintettet írásban, vagy ha az érintett kérelmet elektronikus úton nyújtotta be, elektronikus úton értesíteni kell. A tájékoztatást az Infotv. 15. § (1) bekezdése szerint könnyen hozzáférhető és olvasható formában, lényegre törő, világos és közérthetően megfogalmazott tartalommal kell teljesíteni. A tájékoztatás ingyenes, ha a tájékoztatást kérő a folyó évben azonos adatkörre vonatkozóan tájékoztatási kérelmet még nem nyújtott be. A már megfizetett költségtérítést vissza

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 11 / 18



- kell téríteni, ha az adatokat jogellenesen kezelték vagy a tájékoztatás kérése helyesbítéshez vezetett.
- 2.2. Ha megalapozottan feltehető, hogy az előzőekben meghatározott jogok érvényesítése iránt kérelmet benyújtó személy az érintettel nem azonos személy, a kérelmet az azt benyújtó személy személyazonosságának hitelt érdemlő igazolását követően kell teljesíteni.
 - 2.3. A kérelemre történő adatszolgáltatás szóban, írásban vagy elektronikus úton történhet. A szóban történő adatigénylés esetén az adatszolgáltatási igény regisztrálása adatszolgáltatást igénylő lap útján történik, melyet a kérelmező tölt ki.
 - 2.4. Az adatszolgáltatás iránti kérelmeket iktatni kell és manuális vagy elektronikus úton szükséges nyilvántartani.
 - 2.5. Személyes adat kizárólag akkor szolgáltatatható, amennyiben annak jogszabályi feltételei fennállnak.
 - 2.6. A kérelmező a jogának, vagy jogos érdekének érvényesítéséhez szükséges adat igénylésekor azt a tényt, illetőleg eseményt köteles igazolni, mely biztosítja azt az adatfelhasználási célnak alapot adó kapcsolatot, amely az érintett adat és közötté fennáll vagy fennállt.
 - 2.7. Személyes adatszolgáltatás iránti kérelmet minden osztály kizárólag abban az esetben teljesíthet, ha az igényelt adat a kezelésébe tartozik.
 - 2.8. Közérdekű adatra és közérdekből nyilvános adatra vonatkozó adatigénylés - ide értve az önkormányzat gazdálkodására vonatkozó adatokat is - a közérdekű adatok megismerésére irányuló igények teljesítésének rendjéről szóló szabályzat rendelkezései alapján kell teljesíteni.
 - 2.9. A személyes és a közérdekű adat ütközése esetén a személyes adatok védelméhez való alapjogot és a közérdekű adatok megismeréséhez fűződő alapjogot egymásra tekintettel kell értelmezni, és mindig a vizsgált kérdés tárgyára figyelemmel kell megállapítani e két alapjog hierarchiáját.
 - 2.10. Amennyiben az adatigénylés jogszerűsége, teljesíthetősége vagy ehhez kapcsolódó más körülmény vonatkozásában kétség merül fel, minden adatkezelő köteles a belső adatvédelmi felelős (adatvédelmi tisztviselő) véleményét kikérni, aki 3 napon belül köteles segítséget nyújtani a kétséges körülmények tisztázásához.
 - 2.11. A kérelmező az adatszolgáltatás teljesítéséig kérelmét bármikor visszavonhatja.
 - 2.12. Az adatszolgáltatási nyilvántartásból minden osztály az elutasított kérelmekről, valamint az elutasítás indokairól minden évben január 15. napjáig összesített jelentést készít a belső adatvédelmi felelős (adatvédelmi tisztviselő) részére. A belső adatvédelmi felelős (adatvédelmi tisztviselő) az osztályok által továbbított jelentést összesíti, és január 31-éig tájékoztatja a Nemzeti Adatvédelmi és

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 12 / 18



Információszabadság Hatóságot.

- 2.13. Az adatbetekintéssel kapcsolatos eljárásra az adatszolgáltatási eljárás szabályai értelemszerűen irányadók.
- 2.14. A kép- és hanganyaggal kapcsolatos betekintés rendjére az iratanyagra vonatkozó szabályokat kell alkalmazni. Az adatszolgáltatással kapcsolatban felmerülő költségértékes mértéke megegyezik a közérdekű adatok igénylésének díjával.
- 2.15. Ha az érintett kérelme a kezelt személyes adatok helyesbítésére, törlésére vagy ezen adatok kezelésének korlátozására elutasításra kerül, erről az érintettet írásban haladéktalanul tájékoztatni kell az Infotv. 21. §-ában meghatározott feltételekkel. Az érintett a törlés jogával nem élhet, ha az adatok kezelése az Infotv. 5. § (1) bekezdés a) vagy c) pontján, vagy (2) bekezdés b) pontján alapul.

3. Közérdekű adatok nyilvánossága

- 3.1. A közérdekű adatokat a hivatal (a személyes és a minősített, illetve az Infotv. vagy egyéb törvény által más okból korlátozott megismerhetőségű adatok kivételével) honlapján és a helyi médiában rendszeresen közzéteszi.
- 3.2. A hivatal által bármilyen formában nyilvánosságra hozott dokumentumot lehetőség szerint elektronikus úton is közre kell bocsátani.
- 3.3. 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 és a polgármester előzetes tájékoztatása és egyetértése mellett – minden köztisztviselő köteles pontosan és haladéktalanul eleget tenni.

IV. fejezet

A képviselő-testületi ülésekkel, bizottsági ülésekkel kapcsolatos iratanyag kezelésére vonatkozó külön szabályok

1. A képviselő-testületi és a bizottsági ülések jegyzőkönyveit, valamint a képviselő-testületi határozatokat az Intézményirányító és Szervezési Osztály tartja nyilván. A polgármesteri határozatokat az az osztály tartja nyilván, akinek a feladatkörébe tartozik az ügyviteli és döntés-előkészítő tevékenység. A vezetői értekezlet feljegyzéseit a jegyzői titkárság titkársági munkatársa tartja nyilván, illetve kezeli az ezzel kapcsolatos iratanyagot.
2. A képviselő-testületi ülések jegyzőkönyveinek és a határozatoknak a naprakész nyilvántartásáért az Intézményirányító és Szervezési Osztály vezetője a felelős.
3. A képviselő-testületi és a bizottsági jegyzőkönyvekbe történő betekintés rendjét az Önkormányzat Szervezeti és Működési Szabályzata tartalmazza.
4. A zárt ülések jegyzőkönyveiből, a zárt ülésen tárgyalt napirendi pontokkal érintett jegyzőkönyvi részekből kizárólag a helyi önkormányzati képviselők és a bizottsági tagok

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 13 / 18



részére teljesíthető adat- szolgáltatás, illetőleg engedélyezhető a betekintési jog gyakorlása. E rendelkezések nem vonatkoznak a közérdekű adat, és a közérdekből nyilvános adatok körére. A közérdekű adat és közérdekből nyilvános adat megismerésének lehetőségét zárt ülés tartása esetén is biztosítani kell.

5. A zárt ülések napirendje - előterjesztése, jegyzőkönyve - kizárólag a képviselő-testületi tagok és a bizottsági tagok részére kézbesíthető.
6. A média - írott és elektronikus sajtó -, a könyvtár, illetőleg más külső személy vagy szerv részére kézbesítendő előterjesztés, jegyzőkönyv nem tartalmazhat személyes adatot.
7. A testületi ülésekkel kapcsolatos iratanyag kezelésére vonatkozóan egyebekben az iratkezelési szabályzat rendelkezései az irányadók.
8. A testületi ülésekre vonatkozó előterjesztések kézbesítése az Interneten keresztül, vagy kérésre papír alapon történik, a hozzáférési jogosultságok személyre szólóan vannak meghatározva.

V. fejezet

Az információbiztonság vonatkozásai az adatvédelemben és adatbiztonságban

A hivatali munkavégzés során a szervezeti folyamatok minden szintjén megjelennek mind az információbiztonsággal (adatbiztonsággal), mind pedig az adatvédelemmel kapcsolatos követelmények.

2016. szeptember 3-án lépett hatályba az önkormányzati ASP rendszerről szóló 257/2016. (VIII. 31.) Korm. rendelet, amely előírja, hogy csak az az önkormányzat csatlakozhat az ASP rendszerhez, amely teljesíti a Rendeletben megfogalmazott informatikai és információbiztonsági követelményeket, amelyeket a Rendelet 2. számú melléklete tartalmaz.

„Elvárt informatikai biztonsági megfelelés:

Az állami és önkormányzati szervek elektronikus információbiztonságáról történő megfelelésről szóló 2013. évi L. törvény, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet rendelkezéseiből következő, a rendszer biztonsági osztályba sorolása alapján megállapított információbiztonsági követelményeknek történő megfelelés.”

Ennek értelmében a hivatalnak az ASP szakrendszerek biztonsági osztályba sorolása alapján megállapított információbiztonsági követelményeit a reá vonatkozó mértékben teljesítenie kell (amelyet a MÁK és a Kincsinfo által kiadott *Tájékoztató az önkormányzati ASP rendszerekhez csatlakozáshoz megvalósítandó informatikai biztonsági követelményekről* dokumentum tartalmaz). Rendelkeznie kell Informatikai Biztonsági Szabályzattal (illetve annak kapcsolódó dokumentumaival), amelyben a meghatározott biztonsági követelményeket (adminisztratív, fizikai és logikai védelmi intézkedések) a hivatal egészére, annak minden folyamatára érvényesíteni szükséges.

A **Sajószentpéteri Polgármesteri Hivatal** a mindenkor aktuális *Informatikai Biztonsági Szabályzatában* határozta meg az adminisztratív, fizikai és logikai védelmi intézkedéseket, amely intézkedések és szabályok elősegítik az adatvédelem és adatbiztonság biztosítását is,

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 14 / 18



azonban e mellett szükséges figyelembe venni és érvényesíteni az adatvédelem és adatbiztonsággal kapcsolatos jogszabályi előírásokat.

Az Informatikai Biztonsági Szabályzat (és ezzel együtt az adatvédelem céljából létrehozott és dokumentált szabályok, eljárások) követésének és betartásának, illetve betartatásának az adatvédelem elősegítésében is fontos szerepe van, hiszen ebben az esetben is megjelenik az információbiztonságban már jól ismert 3 alapelv: bizalmasság, sértetlenség és rendelkezésre állás.

Adatvédelem a GDPR-ban

(26) preambulium

Az adatvédelem elveit minden azonosított vagy azonosítható természetes személyre vonatkozó információ esetében alkalmazni kell. Az álnevesített személyes adatok, amelyeket további információ felhasználásával valamely természetes személlyel kapcsolatba lehet hozni, azonosítható természetes személyre vonatkozó adatnak kell tekinteni. Valamely természetes személy azonosíthatóságának meghatározásakor minden olyan módszert figyelembe kell venni – ideértve például a megjelölést –, amelyről észszerűen feltételezhető, hogy az adatkezelő vagy más személy a természetes személy közvetlen vagy közvetett azonosítására felhasználhatja.

Annak meghatározásakor, hogy mely eszközökről feltételezhető észszerűen, hogy egy adott természetes személy azonosítására fogják felhasználni, az összes objektív tényezőt figyelembe kell venni, így például az azonosítás költségeit és időigényét, számításba véve az adatkezeléskor rendelkezésre álló technológiákat, és a technológia fejlődését. **Az adatvédelem elveit ennek megfelelően az anonim információkra nem kell alkalmazni,** nevezetesen olyan információkra, amelyek nem azonosított vagy azonosítható természetes személyre vonatkoznak, valamint az olyan személyes adatokra, amelyeket olyan módon anonimizáltak, amelynek következtében az érintett nem vagy többé nem azonosítható. **Ez a rendelet ezért nem vonatkozik az ilyen anonim információk kezelésére, a statisztikai vagy kutatási célú adatkezelést is ideértve.**

(78) preambulium

A természetes személyeket személyes adataik kezelése tekintetében megillető jogok és szabadságok védelme megköveteli az e rendelet követelményeinek teljesítését biztosító megfelelő technikai és szervezési intézkedések meghozatalát. Ahhoz, hogy az adatkezelő igazolni tudja az e rendeletnek való megfelelést, olyan belső szabályokat kell alkalmaznia, valamint olyan intézkedéseket kell végrehajtania, amelyek teljesítik különösen a beépített és az alapértelmezett adatvédelem elveit. Az említett intézkedések magukban foglalhatják a személyes adatok kezelésének minimálisra csökkentését, a személyes adatok mihamarabbi álnevesítését, a személyes adatok funkcióinak és kezelésének átláthatóságát, valamint azt, hogy az érintett nyomon követhesse az adatkezelést, az adatkezelő pedig biztonsági elemeket hozhasson létre és továbbfejleszthesse azokat.

Az olyan alkalmazások, szolgáltatások és termékek kifejlesztésekor, tervezésekor, kiválasztásakor és felhasználásakor, amelyek személyes adatok kezelésén alapulnak vagy rendeltetésük teljesítéséhez személyes adatokat kezelnek, a termékek, szolgáltatások és alkalmazások előállítóit arra kell ösztönözni, hogy e termékek, szolgáltatások és alkalmazások kifejlesztésekor és tervezésekor szem előtt tartsák a személyes adatok védelméhez való jogot, és a tudomány és technológia állását kellően figyelembe véve

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 15 / 18



gondoskodjanak arról, hogy az adatkezelők és az adatfeldolgozók adatvédelmi kötelezettségeiknek eleget tegyenek. **A beépített és az alapértelmezett adatvédelem elveit a közbeszerzések során is figyelembe kell venni.**

(108) preambulium

Megfelelőségi határozat hiányában az adatkezelő vagy az adatfeldolgozó a megfelelő garanciák érintett számára való biztosítása útján gondoskodik az adatvédelem harmadik országbeli hiányosságainak ellensúlyozásáról. Ezek a megfelelő garanciák magukban foglalhatják a kötelező erejű vállalati szabályok, a Bizottság által elfogadott általános adatvédelmi kikötések, a felügyeleti hatóság által elfogadott általános adatvédelmi kikötések vagy a felügyeleti hatóság által engedélyezett általános szerződési feltételek alkalmazását. **A garanciák biztosítják az adatvédelmi követelményeknek való megfelelést, és az Unión belüli adatkezelés esetén biztosított jogokkal azonos szintű jogokat biztosítanak az érintettek számára, beleértve az érintettek jogainak érvényesíthetőségét és a hatékony jogorvoslat lehetőségét, ezen belül ideértve azt, hogy az érintettek hatékony közigazgatási vagy bírósági jogorvoslatot vehessenek igénybe és kártérítést igényelhessenek az Unióban vagy egy harmadik országban.** A garanciák különösen a személyes adatok kezelésre vonatkozó általános elveknek, valamint a beépített és alapértelmezett adatvédelem elveinek való megfelelésre vonatkoznak. Adattovábbítást közhatalmi szerv vagy egyéb, közfeladatot ellátó szervek is végezhetnek, harmadik országbeli közhatalmi szervek vagy egyéb, közfeladatot ellátó szervek vagy hasonló feladatot vagy funkciókat ellátó nemzetközi szervezetek felé, ideértve a közigazgatási megállapodásokba – például egyetértési megállapodás formájában – beillesztendő, az érintetteknek tényleges és érvényesíthető jogokat biztosító rendelkezések alapján. Az illetékes felügyeleti hatóság engedélyét be kell szerezni abban az esetben, ha a garanciákat olyan közigazgatási megállapodások tartalmazzák, amelyek jogilag nem kötelező erejűek.

(114) preambulium

Ha a Bizottság az adott harmadik ország viszonylatában nem hozott határozatot a harmadik ország adatvédelmi szintjéről, az adatkezelő vagy az adatfeldolgozó olyan megoldásokhoz folyamodhat, amelyek az érintettek számára olyan tényleges és érvényesíthető jogokat garantálnak, hogy az érintettek az adattovábbítást követően is élvezhetik az őket megillető alapvető jogokat és garanciákat.

25. cikk Beépített és alapértelmezett adatvédelem

(1) Az adatkezelő a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, **változó valószínűségű és súlyosságú kockázat figyelembevételével mind az adatkezelés módjának meghatározásakor, mind pedig az adatkezelés során olyan megfelelő technikai és szervezési intézkedéseket – például álnevesítést – hajt végre, amelyek célja egyrészt az adatvédelmi elvek, például az adattakarékosság hatékony megvalósítása, másrészt az e rendeletben foglalt követelmények teljesítéséhez és az érintettek jogainak védelméhez szükséges garanciák beépítése az adatkezelés folyamatába.**

(2) Az adatkezelő megfelelő technikai és szervezési intézkedéseket hajt végre annak biztosítására, hogy **alapértelmezés szerint kizárólag olyan személyes adatok kezelésére kerüljön sor, amelyek az adott konkrét adatkezelési cél szempontjából szükségesek.** Ez a kötelezettség vonatkozik a gyűjtött személyes adatok mennyiségére, kezelésük mértékére, tárolásuk időtartamára és hozzáférhetőségükre. Ezek az intézkedések különösen azt kell, hogy

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 16 / 18



biztosítsák, hogy a személyes adatok alapértelmezés szerint a természetes személy beavatkozása nélkül ne válhassanak hozzáférhetővé meghatározatlan számú személy számára.

32. cikk Az adatkezelés biztonsága

(1) Az adatkezelő és az adatfeldolgozó a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, **változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja**, ideértve, többek között, adott esetben:

- a) a személyes adatok álnevesítését és titkosítását;
- b) a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítását, integritását, rendelkezésre állását és ellenálló képességét;
- c) fizikai vagy műszaki incidens esetén az arra való képességet, hogy a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását kellő időben vissza lehet állítani;
- d) az adatkezelés biztonságának garantálására hozott technikai és szervezési intézkedések hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárást.

(2) A biztonság megfelelő szintjének meghatározásakor kifejezetten figyelembe kell venni az adatkezelésből eredő olyan kockázatokat, amelyek különösen a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítéséből, elvesztéséből, megváltoztatásából, jogosulatlan nyilvánosságra hozatalából vagy az azokhoz való jogosulatlan hozzáférésekből erednek.

(3) Az adatkezelő, illetve az adatfeldolgozó 40. cikk szerinti jóváhagyott magatartási kódexekhez vagy a 42. cikk szerinti jóváhagyott tanúsítási mechanizmushoz való csatlakozását felhasználhatja annak bizonyítása részeként, hogy az e cikk (1) bekezdésében meghatározott követelményeket teljesíti.

(4) Az adatkezelő és az adatfeldolgozó intézkedéseket hoz annak biztosítására, hogy az adatkezelő vagy az adatfeldolgozó irányítása alatt eljáró, a személyes adatokhoz hozzáféréssel rendelkező természetes személyek kizárólag az adatkezelő utasításának megfelelően kezelhessék az említett adatokat, kivéve, ha az ettől való eltérésre uniós vagy tagállami jog kötelezi őket.

A GDPR általános adatvédelmi elvei:

5. cikk A személyes adatok kezelésére vonatkozó elvek

(1) A személyes adatok:

- a) kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni („**jogszerűség, tisztességes eljárás és átláthatóság**”);
- b) gyűjtése csak meghatározott, egyértelmű és jogszerű célból történjen, és azokat ne kezeljék ezekkel a célokkal össze nem egyeztethető módon; a 89. cikk (1) bekezdésének megfelelően nem minősül az eredeti céllal össze nem egyeztethetőnek a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból történő további adatkezelés („**célhoz kötöttség**”);

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 17 / 18



c) az adatkezelés céljai szempontjából megfelelőek és relevánsak kell, hogy legyenek, és a szükségesre kell korlátozódniuk („**adattakarékosság**”);

d) pontosnak és szükség esetén naprakésznek kell lenniük; minden észszerű intézkedést meg kell tenni annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul töröljék vagy helyesbítsék („**pontosság**”);

e) tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé; a személyes adatok ennél hosszabb ideig történő tárolására csak akkor kerülhet sor, amennyiben a személyes adatok kezelésére a 89. cikk (1) bekezdésének megfelelően közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból kerül majd sor, az e rendeletben az érintettek jogainak és szabadságainak védelme érdekében előírt megfelelő technikai és szervezési intézkedések végrehajtására is figyelemmel („**korlátozott tárolhatóság**”);

f) kezelését oly módon kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve („**integritás és bizalmas jelleg**”).

(2) Az adatkezelő felelős az (1) bekezdésnek való megfelelésért, továbbá képesnek kell lennie e megfelelés igazolására („**elszámoltathatóság**”).

VI. fejezet

Záró rendelkezések

1. Az adatvédelmi és adatbiztonsági szabályzatban meghatározott feladatokat, illetőleg jogosultságokat a munkaköri leírásokban fel kell tüntetni.
2. Ez a szabályzat 2018. május 15. napján lép hatályba, ezzel egyidejűleg hatályát veszti a 3/2015. számú adatvédelmi és adatbiztonsági szabályzat.

Sajószentpéter, 2018. augusztus 15.

Dr. Faragó Péter

polgármester



Dr. Guláné Bacsó Krisztina

jegyző



Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 18 / 18