Börcs Község Önkormányzata
ADATVÉDELMI SZABÁLYZAT

Verzió	2.0
Kiadás dátuma	2026. június 1.
Állapot	Hatályos

Változás jegyzék

Verziószám	Kiadási dátum	Leírás
1.0	2024. február 1.	Első kiadás
2.0	2026. június 1.	Hatályosítás, szerkezeti átdolgozás

Börcs, 2026. június 1.

Rácz Róbert
polgármester

BÖRCS KÖZSÉG ÖNKORMÁNYZATA * 1.

Dokumentumvezérlés

Mező	Tartalom
Dokumentum megnevezése	Adatvédelmi Szabályzat
Adatkezelő	Börcs Község Önkormányzata
Jóváhagyó / kiadó	Rácz Róbert polgármester
Hatálybalépés	2026. június 1.
Felülvizsgálat	Évente dokumentált megfelelőségi áttekintés; teljes felülvizsgálat legalább kétévente és rendkívüli esemény esetén
Dokumentumgazda	Rácz Róbert polgármester
Szakmai véleményező	Adatvédelmi tisztviselő

Tartalomjegyzék

I. ÁLTALÁNOS RENDELKEZÉSEK

1. A szabályzat célja és jogszabályi környezete

(1) A szabályzat célja, hogy Börcs Község Önkormányzata (a továbbiakban: Önkormányzat vagy Adatkezelő) önálló adatkezelői tevékenységeiben meghatározza a személyes adatok jogszerű, tisztességes, átlátható és biztonságos kezelésének szervezeti és eljárási kereteit.

(2) A szabályzatot az Európai Parlament és a Tanács (EU) 2016/679 rendeletével (GDPR), az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvénnyel (Infotv.), az alkalmazandó ágazati jogszabályokkal, valamint az Önkormányzat iratkezelési és információbiztonsági szabályozásával összhangban kell alkalmazni.

(3) Az Önkormányzat az e szabályzatban nem részletezett technikai és információbiztonsági követelményeket külön Informatikai Biztonsági Szabályzatban (IBSZ), az adatvédelmi incidensek részletes kezelését külön Adatvédelmi Incidenskezelési Eljárásrendben szabályozza.

(4) A szabályzat nem helyettesíti az egyes adatkezelésekre vonatkozó adatkezelési tájékoztatókat, adatkezelési nyilvántartást, adatfeldolgozói szerződéseket, érdekmérlegelési teszteket, adatvédelmi hatásvizsgálatokat vagy ágazati eljárásrendeket.

Jogforrás / szakmai alap: GDPR 5. cikk, 24–25. cikk, 32. cikk; Infotv. 2. §; Mötv. 41. § (1)–(2) bekezdés.

2. A szabályzat hatálya

(1) A szabályzat szervezeti hatálya kizárólag az Önkormányzatra, mint a Mötv. 41. § (1) bekezdése szerinti jogi személyre terjed ki.

(2) A szabályzat nem terjed ki az önkormányzati költségvetési szerveire, az önkormányzati intézmények, gazdasági társaságok, társulások vagy más önálló jogalanyok saját adatkezelői tevékenységeire. E szervezetek adatkezelői minőségét és kötelezettségeit saját szabályozásukban kell rendezni.

(3) A szabályzat személyi hatálya kiterjed a polgármesterre, alpolgármesterre, önkormányzati képviselőkre, bizottsági tagokra, az Önkormányzat által közvetlenül foglalkoztatott személyekre, valamint minden olyan személyre, aki az Önkormányzat nevében vagy utasítása alapján személyes adatot kezel.

(4) A hivatal foglalkoztatottjára e szabályzat annyiban alkalmazandó, amennyiben az Önkormányzat feladatának végrehajtása során az Önkormányzat adatkezelői döntései és utasításai alapján jár el. Ez nem érinti a hivatal saját adatkezelői felelősségét.

(5) A szabályzat tárgyi hatálya kiterjed az Önkormányzat által önállóan vagy más adatkezelővel közösen végzett, részben vagy egészben automatizált adatkezelésekre, továbbá a nyilvántartási rendszer részét képező nem automatizált adatkezelésekre.

(6) A minősített adatok, valamint a GDPR tárgyi hatályán kívül eső különleges célú adatkezelések kezelésére az alkalmazandó külön jogszabályok irányadók. A hatály kérdését adatkezelésenként dokumentáltan kell megvizsgálni.

Jogforrás / szakmai alap: GDPR 2. cikk (1)–(2) bekezdés; Mötv. 41. §; EDPB 07/2020 iránymutatás az adatkezelő és adatfeldolgozó fogalmáról.

3. Az Adatkezelő adatai

Adat	Kitöltendő tartalom
Teljes név	Börcs Község Önkormányzata
Székhely	9152 Börcs, Erzsébet tér 4.
Törzskönyvi azonosító	370158
Adószám	15370158-2-08
Képviseli	Rácz Róbert polgármester
Központi elérhetőség	+36 96 553 240; polgarmester@borcs.hu; https://borcs.hu/
Adatvédelmi tisztviselő	dr. Szalay Péter
DPO elérhetősége	+36 30 216 5798; borcs@peterszalay.hu

(1) Az adatvédelmi tisztviselő elérhetőségét az Önkormányzat közzéteszi, és a GDPR 37. cikk (7) bekezdése szerint közli a Nemzeti Adatvédelmi és Információszabadság Hatósággal.

Jogforrás / szakmai alap: GDPR 13. cikk (1) bekezdés a)–b) pont; 37. cikk (7) bekezdés.

4. Fogalmak és értelmezési szabályok

(1) A szabályzatban használt fogalmakat elsősorban a GDPR 4. cikke, az Infotv. 3. §-a és az alkalmazandó ágazati jogszabályok szerint kell értelmezni.

- adatkezelési folyamatgazda: az a kijelölt tisztségviselő, szervezeti kapcsolattartó vagy feladatfelelős, aki az adott önkormányzati adatkezelés célját, működését, adattartalmát és gyakorlati végrehajtását ismeri, és az adatkezelői döntések előkészítéséért felel
- felhatalmazott személy: az Önkormányzat vagy adatfeldolgozó közvetlen irányítása alatt eljáró személy, aki kizárólag a kapott utasítás és hozzáférési jogosultság keretei között kezelhet személyes adatot
- adatvédelmi dokumentáció: különösen az adatkezelési nyilvántartás, tájékoztató, szerződés, hatásvizsgálat, érdekmérlegelési teszt, incidensnyilvántartás, kérelemnyilvántartás és a megfelelést igazoló egyéb irat
- különleges célú adatkezelés: olyan adatkezelés, amelynek GDPR vagy Infotv. szerinti jogi rezsimjét az adatkezelés céljára és az eljáró szerv feladataira tekintettel külön kell meghatározni

Jogforrás / szakmai alap: GDPR 4. cikk, 29. cikk; Infotv. 3. §.

5. Adatkezelési alapelvek

(1) Jogszerűség, tisztességes eljárás és átláthatóság: az adatkezelés jogalapja, célja és lényeges körülményei előzetesen meghatározottak és az érintett számára megismerhetők.

(2) Célhoz kötöttség: személyes adat csak meghatározott, egyértelmű és jogszerű célból kezelhető; új célú felhasználás előtt összeegyeztethetőségi és jogalapvizsgálat szükséges.

(3) Adattakarékosság: csak a cél eléréséhez megfelelő, releváns és szükséges adat kezelhető.

(4) Pontosság: a pontatlan adatot indokolatlan késedelem nélkül helyesbíteni vagy törölni kell, figyelemmel az irat hitelességére és az archiválási kötelezettségre.

(5) Korlátozott tárolhatóság: a megőrzési időt adatkezelésenként, jogszabály, irattári terv, cél, elévülési idő és dokumentált kockázat alapján kell meghatározni.

(6) Integritás és bizalmas jelleg: kockázatarányos technikai és szervezési intézkedésekkel kell védeni az adatokat.

(7) Elszámoltathatóság: az Önkormányzatnak nemcsak meg kell felelnie, hanem képesnek kell lennie a megfelelés igazolására.

Jogforrás / szakmai alap: GDPR 5. cikk (1)–(2) bekezdés; 24. cikk.

II. AZ ADATKEZELÉS IRÁNYÍTÁSA ÉS FELELŐSSÉGI RENDSZERE

6. Az adatkezelői döntéshozatal

(1) Az adatkezelés céljairól és lényeges eszközeiről az Önkormányzat dönt. A döntési hatáskört az Mötv., az Önkormányzat szervezeti és működési szabályzata, a képviselő-testület döntései és az átruházott hatáskörök rendje alapján kell meghatározni.

(2) A jelen szabályzat jóváhagyására és kiadására jogosult szervet vagy személyt az Önkormányzat szervezeti és működési szabályzata, illetve hatásköri rendje alapján kell kiválasztani. A szabályzatot a polgármester átruházott hatáskör alapján kiadja.

(3) Az adatkezelői döntésnek dokumentálhatónak kell lennie. A DPO véleménye nem helyettesíti az adatkezelő döntését, és a DPO nem utasítható arra, hogy az adatkezelő helyett kockázatot fogadjon el.

Jogforrás / szakmai alap: GDPR 4. cikk 7. pont, 24. cikk; Mötv. 41. § (1), (3)–(4) bekezdés, 65. §; EDPB 07/2020 iránymutatás.

7. Felelősségi szerepkörök

Szerepkör	Fő felelősség
Képviselő-testület	Az adatkezeléshez kapcsolódó önkormányzati döntések meghozatala a jogszabályi és belső hatásköri rend szerint; szükséges erőforrások biztosítása.
Polgármester	Az Önkormányzat törvényes képviselete; a szabályzat végrehajtásának vezetői biztosítása; az adatkezelői döntések meghozatala a saját vagy átruházott hatáskörében.
Adatkezelési folyamatgazda	Az adatkezelés leírása, jogalap- és célvizsgálat kezdeményezése, nyilvántartási adatok naprakészen tartása, tájékoztató és megőrzési szabályok működtetése, kérelem és incidens azonnali továbbítása.
Adatvédelmi koordinátor / dokumentumgazda	A dokumentáció és feladatlista koordinációja, határidők követése, döntés-előkészítés
Adatvédelmi tisztviselő	Tájékoztatás, tanácsadás, megfelelőség-ellenőrzés, DPIA-val kapcsolatos tanácsadás és ellenőrzés, hatósági kapcsolattartás; független, utasítástól mentes működés.
Felhatalmazott személy	Csak dokumentált feladat, utasítás és jogosultság alapján kezelhet adatot; titoktartási, biztonsági és incidensjelentési kötelezettség terheli.
Informatikai üzemeltető / szolgáltató	Az IBSZ és szerződés szerinti technikai intézkedések végrehajtása, naplózás, mentés, hozzáférés-kezelés, sérülékenység- és incidenskezelési támogatás.

(1) A szerepkörök személyhez rendelését és helyettesítését az 1. melléklet szerinti szerepkör- és felelősségi mátrixban kell dokumentálni.

Jogforrás / szakmai alap: GDPR 24. cikk, 29. cikk, 37–39. cikk; WP29/EDPB DPO-iránymutatás WP243 rev.01.

8. Az adatvédelmi tisztviselő jogállása

(1) Az Önkormányzat mint közhatalmi szerv adatvédelmi tisztviselőt jelöl ki. A DPO kijelölése történhet munkaviszony vagy szolgáltatási szerződés alapján, egyénileg vagy – a hozzáférhetőség és erőforrások biztosítása mellett – több szerv számára közösen.

(2) A DPO-t valamennyi, személyes adatok védelmével kapcsolatos ügybe megfelelő időben be kell vonni, és számára biztosítani kell a feladatai ellátásához szükséges hozzáférést, erőforrásokat, szakmai továbbképzést és közvetlen felső vezetői beszámolási lehetőséget.

(3) A DPO feladatai ellátásával kapcsolatban utasítást nem kaphat. Más feladata csak akkor lehet, ha az nem eredményez összeférhetetlenséget, különösen nem jár az adatkezelés céljainak és eszközeinek meghatározásával.

(4) A DPO tanácsától eltérő adatkezelői döntést indokolással kell dokumentálni, ha az eltérés jelentős adatvédelmi kockázatot érint.

Jogforrás / szakmai alap: GDPR 37. cikk (1) bekezdés a) pont, 37. cikk (3), (5)–(7) bekezdés; 38–39. cikk; WP243 rev.01.

III. ADATKEZELÉSI KÖVETELMÉNYEK ÉS ELJÁRÁSOK

9. Új vagy módosuló adatkezelés engedélyezése

(1) Személyes adatot érintő új folyamat, szolgáltatás, informatikai rendszer, űrlap, nyilvántartás, kamerarendszer, online közzététel, adattovábbítás vagy beszállítói szolgáltatás csak dokumentált adatvédelmi előzetes vizsgálat után vezethető be.

- 1. a cél és az adatkezelői szerep meghatározása
- 2. az érintettek, adatkategóriák, adatforrások és címzettek feltárása
- 3. a GDPR szerinti jogalap és – különleges adat esetén – a 9. cikk szerinti feltétel meghatározása
- 4. az adattakarékosság, megőrzési idő és hozzáférési kör megállapítása
- 5. az érintetti tájékoztatás és joggyakorlás megtervezése
- 6. adatfeldolgozó, közös adatkezelő vagy önálló adatkezelő partner minősítése
- 7. adatbiztonsági és nemzetközi adattovábbítási vizsgálat
- 8. DPIA-szükségességi előszűrés
- 9. a DPO megfelelő időben történő bevonása
- 10. az adatkezelési nyilvántartás és kapcsolódó dokumentumok jóváhagyása

(2) Az előzetes vizsgálatot a melléklet szerinti új adatkezelési adatlap dokumentálja. Az adatkezelés csak a kijelölt döntéshozó írásbeli jóváhagyása után kezdhető meg.

Jogforrás / szakmai alap: GDPR 5. cikk (2) bekezdés, 24–25. cikk, 30. cikk, 35–36. cikk.

10. Az adatkezelés jogalapja

(1) Minden adatkezelési célhoz külön, a tényleges körülményeknek megfelelő GDPR 6. cikk (1) bekezdése szerinti jogalapot kell meghatározni. A jogalapot nem lehet utólag, kizárólag a már kialakított gyakorlat igazolása érdekében megválasztani.

Jogalap	Alkalmazási követelmény
GDPR 6. cikk (1) c)	Az Önkormányzatra alkalmazandó uniós vagy magyar jogi kötelezettség teljesítése. A nyilvántartásban meg kell jelölni a kötelezettséget előíró konkrét jogszabályhelyet.
GDPR 6. cikk (1) e)	Közérdekű vagy az Önkormányzatra ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat. Meg kell jelölni a feladatot meghatározó uniós vagy magyar jogalapot.
GDPR 6. cikk (1) b)	Olyan szerződés teljesítése vagy az érintett kérésére szerződéskötést megelőző lépések, amelyben az érintett fél.
GDPR 6. cikk (1) a)	Önkéntes, konkrét, tájékozott és egyértelmű hozzájárulás; közhatalmi vagy alá-fölérendeltségi helyzetben csak kivételesen, valódi választási lehetőség esetén.
GDPR 6. cikk (1) d)	Az érintett vagy más természetes személy létfontosságú érdekeinek védelméhez szükséges, tipikusan rendkívüli

Jogalap	Alkalmazási követelmény
	esetben.
GDPR 6. cikk (1) f)	Az Önkormányzat közfeladatainak ellátása során nem alkalmazható. Csak dokumentáltan elkülönülő, nem közhatalmi tevékenységnél, érdekmérlegelési teszt alapján jöhet szóba.

(2) Különleges személyes adat kezelése esetén a GDPR 6. cikke szerinti jogalap mellett a GDPR 9. cikk (2) bekezdésének megfelelő feltételt és az alkalmazandó jogszabályi garanciákat is dokumentálni kell. Büntetőjogi felelősségre vonatkozó adat kizárólag a GDPR 10. cikkében és a magyar jogban meghatározott feltételekkel kezelhető.

Jogforrás / szakmai alap: GDPR 6. cikk, különösen 6. cikk (1) bekezdés f) pont utolsó albekezdése; 9–10. cikk; Infotv. 5. § az Infotv. különös hatálya alá tartozó adatkezelésekben.

11. Adatkezelési nyilvántartás

(1) Az Önkormányzat az adatkezelői minőségében végzett adatkezelési tevékenységek kategóriáiról elektronikus, naprakész nyilvántartást vezet. Közhatalmi szervként az Önkormányzat nem alkalmazhatja a GDPR 30. cikk (5) bekezdése szerinti kis szervezeti kivételt.

(2) A nyilvántartás minimálisan tartalmazza a GDPR 30. cikk (1) bekezdésében meghatározott adatokat, továbbá az alkalmazhatóság szerint a jogalapot és konkrét jogszabályhelyet, az adatforrást, a különleges adatok feltételét, a tájékoztató azonosítóját, az adatfeldolgozót, az adatkezelői szerepértékelést, a DPIA/LIA állapotát, az informatikai rendszert és a megőrzés jogi indokát.

(3) A folyamatgazda minden lényeges változást előzetesen, sürgős esetben haladéktalanul jelez a dokumentumgazdának és a DPO-nak. A nyilvántartás legalább évente teljes körűen felülvizsgálandó.

Jogforrás / szakmai alap: GDPR 30. cikk; elszámoltathatóság: GDPR 5. cikk (2) bekezdés, 24. cikk.

12. Tájékoztatási kötelezettség

(1) Az érintett részére a GDPR 12–14. cikke szerinti tájékoztatást tömör, átlátható, érthető és könnyen hozzáférhető formában, világos és közérthető nyelven kell megadni.

(2) Az adatkezelési tájékoztatót az adatfelvétel előtt vagy azzal egyidejűleg kell elérhetővé tenni. Nem az érintettől származó adatoknál a GDPR 14. cikk (3) bekezdésében meghatározott időpontban kell tájékoztatni, kivéve, ha dokumentált kivétel alkalmazható.

(3) A tájékoztató nem tartalmazhat általános, valótlan vagy több, egymással helyettesíthető jogalapot. A címzetteket, adatfeldolgozókat, megőrzési időt és érintetti jogokat a tényleges adatkezelés szerint kell bemutatni.

(4) Az Önkormányzat a hatályos tájékoztatókról nyilvántartást vezet, amely tartalmazza a verziót, hatályt, közzétételi helyet, felelőst és felülvizsgálati dátumot.

Jogforrás / szakmai alap: GDPR 12–14. cikk; EDPB/WP29 átláthatósági iránymutatás WP260 rev.01.

13. Az érintetti jogok gyakorlása

(1) Az érintett kérelmét annak elnevezésétől és benyújtási csatornájától függetlenül tartalma szerint kell értékelni. A kérelmet átvevő személy haladéktalanul, de legkésőbb egy munkanapon belül továbbítja a kijelölt koordinátornak és a DPO-nak.

(2) Az Önkormányzat indokolatlan késedelem nélkül, de legkésőbb a kérelem beérkezésétől számított egy hónapon belül tájékoztatja az érintettet az intézkedésről. A határidő a GDPR 12. cikk (3) bekezdése szerinti feltételekkel további két hónappal meghosszabbítható; erről és az okokról az első egy hónapon belül tájékoztatni kell az érintettet.

(3) Személyazonosság igazolása csak megalapozott kétség esetén, a szükséges mértékben kérhető. A rendszeresen kezelt azonosítónál több adatot pusztán a kérelem teljesítése céljából nem szabad gyűjteni.

Jog	Alkalmazás
hozzáférés	GDPR 15. cikk; mások jogainak és szabadságainak védelme mellett
helyesbítés	GDPR 16. cikk; az irat hitelességének megőrzésével, szükség esetén kiegészítő nyilatkozattal
törlés	GDPR 17. cikk; nem abszolút jog, különösen jogi kötelezettség, közfeladat, jogi igény vagy közérdekű archiválás esetén korlátozott
korlátozás	GDPR 18. cikk; a megjelölés és további műveletek kontrollja dokumentálandó
adathordozhatóság	GDPR 20. cikk; csak hozzájáruláson vagy szerződésen alapuló, automatizált adatkezelésnél
tiltakozás	GDPR 21. cikk; különösen a 6. cikk (1) e) vagy f) pontján alapuló adatkezelésnél, a vonatkozó feltételekkel
automatizált döntés	GDPR 22. cikk; az alkalmazhatóságot adatkezelésenként kell vizsgálni

(4) A kérelem teljesítésének vagy elutasításának döntését az adatkezelői hatáskörrel rendelkező személy hozza meg. A DPO tanácsot ad és ellenőriz, de a kérelmet nem saját nevében bírálja el.

(5) A kérelmeket, az elvégzett kereséseket, a döntést, a határidőket, a személyazonosság-ellenőrzést és az átadott másolatokat a szükséges bizonyíthatóság mellett dokumentálni kell.

Jogforrás / szakmai alap: GDPR 12. cikk (2)–(6) bekezdés, 15–22. cikk; 23. cikk szerinti korlátozás csak megfelelő uniós vagy tagállami jog alapján.

14. Adatpontosság, megőrzés, törlés és archiválás

(1) A folyamatgazda meghatározza és dokumentálja az adatfrissítés módját, a megőrzési időt, a felülvizsgálati időpontot és a törlés, anonimizálás, selejtezés vagy levéltári átadás módját.

(2) A megőrzési idő elsődlegesen a konkrét jogszabályból, irattári tervből vagy kötelező archiválási szabályból következik. Ennek hiányában a cél eléréséhez szükséges idő, az alkalmazandó elévülés, a jogi igények és az érintetti kockázatok dokumentált mérlegelése alapján kell meghatározni.

(3) A megőrzési idő lejárta után a személyes adatot biztonságosan törölni, anonimizálni, selejtezni vagy – ha jogszabály és irattári terv előírja – levéltárba adni kell. A törlés nem tehető függővé attól, hogy az az Önkormányzat számára kényelmes vagy előnyös-e.

(4) Az elektronikus törlésnek ki kell terjednie az aktív rendszerekre és az észszerűen kezelhető másolatokra. A biztonsági mentésekben maradó adatokat a mentési ciklus lejártáig el kell zárni a rendes felhasználástól, és a visszaállítási eljárásban biztosítani kell a korábbi törlés ismételt érvényesítését.

(5) Közérdekű archiválás esetén a GDPR 89. cikke szerinti megfelelő garanciákat, így különösen az adattakarékosságot és szükség szerint az álnevesítést alkalmazni kell.

Jogforrás / szakmai alap: GDPR 5. cikk (1) bekezdés d)–e) pont, 17. cikk (3) bekezdés d) pont, 25. cikk, 89. cikk; Ltv.: 335/2005. (XII. 29.) Korm. rendelet; az Önkormányzat hatályos irattári terve.

15. Adattovábbítás, hozzáférhetővé tétel és nyilvánosságra hozatal

(1) Személyes adat címzett részére csak dokumentált célból, megfelelő jogalappal, az adattakarékosság és biztonság követelményeinek betartásával adható át vagy tehető hozzáférhetővé.

(2) Hatósági vagy más szervi megkeresésnél ellenőrizni kell a megkereső személyét, hatáskörét, a konkrét jogalapot, a kért adatkört és az adattovábbítás biztonságos csatornáját. Az adattovábbítást a szükséges mértékben dokumentálni kell.

(3) Telefonon személyes adat kizárólag akkor közölhető, ha az adatátvevő személyazonossága és jogosultsága megfelelően ellenőrizhető, a közlés szükséges és arányos, és a közlés körülményei kizárják vagy elfogadható szintre csökkentik a jogosulatlan megismerés kockázatát. Különleges adat telefonos közlését főszabályként kerülni kell.

(4) Az internetes közzététel önálló adatkezelési művelet. A közérdekből nyilvános adat sem tehető automatikusan korlátlan ideig és korlátlan kereshetőséggel hozzáférhetővé; vizsgálni kell a közzététel konkrét jogalapját, terjedelmét, időtartamát és keresőmotor-indexelési kockázatát.

(5) Harmadik országba vagy nemzetközi szervezet részére történő adattovábbítás előtt a GDPR V. fejezetében meghatározott feltételeket és a szolgáltatói láncot dokumentáltan kell vizsgálni.

Jogforrás / szakmai alap: GDPR 5–6., 13., 21., 25. és 32. cikk; Kttv. 1. § (1) bekezdés a)–b) pont, 177. §, 225/A–225/L. §, 257–258. § – kizárólag az adott jogviszony és szervezeti hatály szerint; Mt., Ptk. és az adott jogviszonyra vonatkozó ágazati szabályok; NAIH munkahelyi adatkezelési tájékoztatója (2016, a GDPR szerint aktualizálandó elvekkel).

16. Adatfeldolgozók és más adatkezelők

(1) A szerződéses partner adatvédelmi szerepét a szolgáltatás megnevezése helyett a tényleges feladatok, döntési jogosultságok, célok és eszközök alapján kell minősíteni. A minősítést az adatkezelői szerepértékelő lapon kell dokumentálni.

(2) Adatfeldolgozó csak akkor vehető igénybe, ha megfelelő garanciákat nyújt a GDPR követelményeinek teljesítésére és az érintettek jogainak védelmére. A kiválasztást előzetes átvilágítással és kockázatarányos időszakos ellenőrzéssel kell alátámasztani.

(3) Az adatfeldolgozói szerződésnek különösen a következőket kell tartalmaznia:

- az adatkezelés tárgya és időtartama
- az adatkezelés jellege és célja
- a személyes adatok típusa és az érintettek kategóriái
- az Önkormányzat jogai és kötelezettségei
- dokumentált utasítás és nemzetközi továbbítás
- titoktartás
- GDPR 32. cikk szerinti biztonság
- további adatfeldolgozók előzetes egyedi vagy általános írásbeli engedélyezése és változásbejelentése
- érintetti jogok támogatása

- incidens, DPIA és előzetes konzultáció támogatása
- adatok visszaadása vagy törlése
- audit és megfelelési információk
- jogellenes utasítás jelzése

(4) Közös adatkezelés esetén a GDPR 26. cikke szerinti megállapodásban átláthatóan meg kell határozni a kötelezettségek megosztását és az érintetti kapcsolattartás rendjét. Önálló adatkezelők közötti adattovábbításnál nem adatfeldolgozói szerződést, hanem a jogalapot, felelősségi határokat és biztonsági feltételeket kell rögzíteni.

Jogforrás / szakmai alap: GDPR 26., 28–29. cikk; EDPB 07/2020 iránymutatás.

17. Adatvédelmi hatásvizsgálat, érdekmérlegelés és előzetes konzultáció

(1) Az új vagy lényegesen módosuló adatkezelésnél a folyamatgazda és a dokumentumgazda DPIA-előszűrést végez. Ha az adatkezelés valószínűsíthetően magas kockázattal jár, vagy a GDPR 35. cikk (3) bekezdése, illetve a NAIH 35. cikk (4) bekezdése szerinti listája alapján kötelező, az Önkormányzat az adatkezelés megkezdése előtt hatásvizsgálatot végez.

(2) A hatásvizsgálat elvégzéséért az Önkormányzat felelős. A DPO tanácsát ki kell kérni, és a DPO figyelemmel kíséri a hatásvizsgálat végrehajtását. A DPO nem lehet az adatkezelői kockázat elfogadója vagy a végső döntéshozó.

(3) A hatásvizsgálatot a kockázat változásakor, továbbá az Önkormányzat által meghatározott rendszeres felülvizsgálati ciklusban újra kell értékelni. A sablon nem állapít meg minden adatkezelésre automatikus hároméves kötelező időt; a felülvizsgálat gyakoriságát a kockázat és változás alapján kell rögzíteni.

(4) Ha a megfelelő intézkedések után is magas fennmaradó kockázat marad, az adatkezelés megkezdése előtt a GDPR 36. cikke szerint előzetesen konzultálni kell a NAIH-hal.

(5) A GDPR 6. cikk (1) bekezdés f) pontjára alapított kivételes adatkezelés előtt írásbeli érdekmérlegelési tesztet kell készíteni. A teszt azonosítja a jogos érdeket, vizsgálja a szükségességet, az érintetti hatást, az észszerű elvárásokat és a garanciákat.

Jogforrás / szakmai alap: GDPR 6. cikk (1) bekezdés f) pont, 35–36. cikk; NAIH GDPR 35. cikk (4) szerinti hatásvizsgálati lista: WP29/EDPB DPIA-iránymutatás WP248 rev.01.

IV. ADATBIZTONSÁG ÉS INCIDENSKEZELÉSI KAPCSOLÓDÁS

18. Adatbiztonsági követelmények

(1) Az Önkormányzat a személyes adatok biztonságát az adatkezelés jellegéhez, hatóköréhez, körülményeihez és céljaihoz, valamint az érintetti jogokra jelentett kockázathoz igazodó technikai és szervezési intézkedésekkel biztosítja.

- jogosultságok szükséges és legkisebb mértéke, személyhez kötött azonosítás és rendszeres felülvizsgálat
- többtényezős hitelesítés a kockázatnak megfelelően, különösen távoli, adminisztratív és felhő-hozzáférésnél
- naplózás, naplóvédelem és események felülvizsgálata
- biztonsági mentés, elkülönítés, helyreállítási próba és üzletmenet-folytonosság
- eszköz-, javítás-, sérülékenység- és kártevővédelem
- titkosítás vagy más megfelelő védelem adattárolásnál és továbbításnál
- papíralapú iratok fizikai védelme, tiszta asztal és biztonságos megsemmisítés
- mobileszközök, távoli munkavégzés, hordozható adathordozók és magáneszközök szabályozása
- beszállítói és felhőszolgáltatási kockázatok kezelése
- intézkedések rendszeres tesztelése, értékelése és dokumentált javítása

(2) A részletes technikai minimumokat, felelősöket és ellenőrzési ciklusokat az IBSZ tartalmazza. Az IBSZ nem csökkentheti az e szabályzatban és a GDPR 32. cikkében meghatározott kockázatalapú követelményeket.

(3) Az adaptáció során külön, írásban kell vizsgálni, hogy a Kibertv. az Önkormányzatra saját tevékenysége, a Kibertv. 2. vagy 3. melléklete szerinti szolgáltatása, hatósági azonosítása, illetve kritikus vagy jelentős szervezeti kijelölése alapján alkalmazandó-e. A települési önkormányzati jogállás önmagában nem jelenti automatikusan a Kibertv. hatályát; a Kibertv. 1. melléklete a település képviselő-testületének hivatalát nevesíti.

(4) Ha az Önkormányzat a Kibertv. hatálya alá tartozik, az IBSZ-ben és a kapcsolódó nyilvántartásokban biztosítani kell különösen az elektronikus információs rendszerek és a kezelt adatok felmérését és osztályozását, a biztonsági osztályba sorolást, a kockázatmenedzsment keretrendszert, a felelősségi rendet, a védelmi intézkedéseket, azok ellenőrzését és a kiberbiztonsági incidensjelentési kötelezettségek teljesítését.

(5) Ha a Kibertv. az Önkormányzatra nem, de a polgármesteri vagy közös önkormányzati hivatalra alkalmazandó, a hivatal saját kötelezettségeit a hivatali IBSZ-ben és incidenseljárásban kell rendezni. A közösen használt infrastruktúra, szolgáltatás vagy adatállomány tekintetében az Önkormányzat és a hivatal között írásbeli felelősségi, együttműködési és értesítési mátrixot kell kialakítani.

(6) A felhatalmazott személy a személyes adatokat kizárólag a kijelölt feladatához szükséges mértékben ismerheti meg. Jelszó, hitelesítési eszköz vagy felhasználói fiók megosztása tilos, kivéve a dokumentált, technikailag elkerülhetetlen szolgáltatásfiókokat, amelyek külön kontroll alatt állnak.

Jogforrás / szakmai alap: GDPR 25. és 32. cikk; GDPR (78), (83) preambulumbekezdés; Kibertv. 1. §, 6. §, 10–11. § és 66. §; 418/2024. (XII. 23.) Korm. rendelet 77–80. §.

19. Adatvédelmi incidensek

(1) A személyes adatok bizalmas jellegének, sértetlenségének vagy rendelkezésre állásának sérülését, illetve annak gyanúját minden érintett személy haladéktalanul, a külön Adatvédelmi Incidenskezelési Eljárásrend szerint jelenti.

(2) Az adatkezelő a bejelentési kötelezettségről kockázatértékelés alapján dönt. A DPO tanácsot ad; a döntés és annak indoka az Önkormányzat felelőssége.

(3) A NAIH részére történő bejelentést – ha az incidens valószínűsíthetően kockázattal jár – indokolatlan késedelem nélkül és lehetőség szerint a tudomásszerzéstől számított 72 órán belül kell megtenni. Magas kockázat esetén az érintetteket is indokolatlan késedelem nélkül tájékoztatni kell, kivéve a GDPR 34. cikk (3) bekezdése szerinti eseteket.

(4) Minden személyesadat-incidenst dokumentálni kell, ideértve a tényeket, hatásokat, kockázatértékelést, döntéseket, intézkedéseket, bejelentéseket és az utólagos javító intézkedéseket akkor is, ha hatósági vagy érintetti bejelentés nem történt.

(5) Az informatikai eseményt egymástól függetlenül kell minősíteni a GDPR szerinti adatvédelmi incidens és – alkalmazhatóság esetén – a Kibertv. szerinti kiberbiztonsági incidens szempontjából. A két fogalom és bejelentési küszöb nem azonos; az egyik eljárás vagy bejelentés nem helyettesíti a másikat.

(6) Ha az Önkormányzat a Kibertv. hatálya alá tartozik, a bejelentésre köteles kiberbiztonsági eseményt a nemzeti kiberbiztonsági incidenskezelő központ (Központ) részére a Kibertv. 66. §-a és a 418/2024. (XII. 23.) Korm. rendelet szerint kell jelenteni. A határidőkövetésnek ki kell terjednie különösen a 24 órán belüli első bejelentésre, a 72 órán belüli eseménybejelentésre és az alkalmazandó zárójelentésre.

(7) Ha az Önkormányzat valamely adatkezelési művelet tekintetében adatfeldolgozóként jár el, az adatvédelmi incidenst az arról való tudomásszerzést követően indokolatlan késedelem nélkül jelenti az adatkezelőnek. A GDPR 28. cikke szerinti szerződésben vagy más jogi aktusban célszerű ennél rövidebb belső határidőt és a minimálisan továbbítandó információkat is meghatározni.

Jogforrás / szakmai alap: GDPR 4. cikk 12. pont, 33. cikk (1)–(2) és (5) bekezdés, 34. cikk; Kibertv. 66. §; 418/2024. (XII. 23.) Korm. rendelet 77–80. §; NAIH GDPR incidens-tájékoztató; EDPB 01/2021 iránymutatás.

V. ELLENŐRZÉS, OKTATÁS ÉS ZÁRÓ RENDELKEZÉSEK

20. Oktatás és tudatosság

(1) A szabályzat személyi hatálya alá tartozó személy a személyes adatokhoz való hozzáférés előtt adatvédelmi és információbiztonsági alapoktatásban részesül, és nyilatkozik a szabályok, titoktartási kötelezettség és incidensjelentési rend megismeréséről.

(2) Az általános oktatást legalább évente, a kockázatos vagy speciális feladatot ellátók szerepköralapú oktatását szükség szerint meg kell ismételni. Rendkívüli oktatást kell tartani lényeges jogszabály-, rendszer- vagy folyamatváltozás, illetve jelentős incidens után.

(3) Az oktatás témáját, időpontját, résztvevőit, teljesítését és szükség szerint az ismeretellenőrzés eredményét dokumentálni kell.

Jogforrás / szakmai alap: GDPR 5. cikk (2) bekezdés, 24. cikk, 32. cikk (4) bekezdés, 39. cikk (1) bekezdés b) pont.

21. Megfelelőség-ellenőrzés és felülvizsgálat

(1) A dokumentumgazda évente dokumentált megfelelőségi áttekintést szervez, amely kiterjed legalább az adatkezelési nyilvántartás, tájékoztatók, adatfeldolgozók, hozzáférések, megőrzési idők, oktatások, érintetti kérelmek, incidensek, DPIA-k és opcionális modulok aktualitására.

(2) A DPO a kockázatok alapján ellenőrzési tervet készíthet, ellenőrzést folytathat, és ajánlást adhat. Az ellenőrzési megállapításokra intézkedési tervet kell készíteni felelőssel és határidővel.

(3) A szabályzat teljes felülvizsgálatát legalább kétévente, továbbá jogszabályváltozás, szervezeti vagy feladatváltozás, új technológia, magas kockázatú adatkezelés, jelentős incidens vagy hatósági/bírósági megállapítás esetén soron kívül el kell végezni.

Jogforrás / szakmai alap: GDPR 24. cikk (1)–(2) bekezdés, 32. cikk (1) bekezdés d) pont, 39. cikk (1) bekezdés b) pont.

22. Záró rendelkezések

(1) Jelen szabályzat 2026.06.01. napján lép hatályba. Hatálybalépésével egyidejűleg az Önkormányzat korábbi 2024.02.01. napján kelt szabályzata hatályát veszti.

(2) A dokumentumgazda gondoskodik a szabályzat közzétételéről vagy belső elérhetővé tételéről, a személyi hatály alá tartozók igazolható megismertetéséről, a változatkezelésről és az archivált verziók megőrzéséről.

Jogforrás / szakmai alap: GDPR 24. cikk; Mötv. és az Önkormányzat SZMSZ-e szerinti jóváhagyási és hatásköri rend.

M-01 – Honlap, sütik és elektronikus űrlapok

(1) Az Önkormányzat honlapján és elektronikus űrlapjain végzett adatkezeléseket a honlap funkciói, a használt szolgáltatók, sütik, beágyazott tartalmak, naplóadatok és adattovábbítások alapján külön nyilvántartásban kell azonosítani.

(2) Nem szükséges technikai sütit csak az érintett GDPR-követelményeknek megfelelő hozzájárulása után lehet elhelyezni vagy olvasni. A hozzájárulás megtagadása nem lehet nehezebb, mint annak megadása; az előre bejelölt vagy pusztán további böngészésre alapított hozzájárulás nem megfelelő.

(3) Az elektronikus űrlap csak a célhoz szükséges adatmezőket tartalmazhatja, egyértelműen jelölve a kötelező és opcionális mezőket. Az űrlaphoz rétegezett adatkezelési tájékoztatót kell kapcsolni.

(4) Külső analitikai, térképi, videós, betűtípus-, CAPTCHA- vagy más beágyazott szolgáltatás csak adatvédelmi és adattovábbítási vizsgálat után alkalmazható.

(5) A honlap üzemeltetőjével, tárhelyszolgáltatójával és űrlapszolgáltatójával fennálló adatvédelmi szerepeket és szerződéseket dokumentálni kell.

Jogforrás / szakmai alap: GDPR 5–7., 12–14., 25., 28., 44–49. cikk; elektronikus hírközlési és sütiszabályok az alkalmazandó magyar jog szerint.

M-02 – Közösségi média

(1) Az Önkormányzat minden közösségimédia-oldalán kijelöli a kezelési és moderációs felelőst, meghatározza a közzétételi célt, a jogalapot, a megőrzést és a beérkező üzenetek ügyintézési rendjét.

(2) A platformszolgáltató és az Önkormányzat adatvédelmi szerepét funkciónként kell értékelni; a platform által nyújtott statisztikai vagy hirdetési eszközök közös adatkezelést vagy önálló adatkezelést is eredményezhetnek.

(3) Ügyintézéshez szükséges személyes adatot nyilvános hozzászólásban nem szabad kérni. A beadványt biztonságos, hivatalos csatornára kell terelni, és a hozzászólásban megjelent felesleges adatot a moderációs szabályok szerint kezelni kell.

(4) A közösségimédia-oldalra önálló, platform-specifikus adatkezelési tájékoztatót kell készíteni, és az oldal elérhető részén közzé kell tenni.

Jogforrás / szakmai alap: GDPR 5–6., 13–14., 25–26. cikk; EDPB 07/2020 iránymutatás; az adott platform mindenkori adatkezelési feltételei.

M-03 – Rendezvények, fénykép- és videófelvételek

(1) Az önkormányzati rendezvényen készített kép- és hangfelvételek célját, jogalapját, tervezett felhasználását, megőrzését, közzétételi felületeit és a felvételkészítő partner szerepét a rendezvény előtt meg kell határozni.

(2) A rendezvény dokumentálása, tömegfelvétel, egyedi portré, gyermekről készült felvétel, sajtófelvétel és hozzájáruláson alapuló promóciós felvétel jogi megítélése eltérő lehet.

(3) A helyszíni tájékoztatásnak jól láthatónak kell lennie, és részletes online vagy papíralapú tájékoztatóhoz kell vezetnie. Esetleges hozzájárulás alkalmazásakor biztosítani kell a tényleges választást és visszavonhatóságot.

(4) A közzétett felvételek időszakos felülvizsgálatáról és az érintetti kérelmek érdemi kezeléséről gondoskodni kell.

Jogforrás / szakmai alap: GDPR 5–7., 12–13., 17., 21. cikk; Ptk. 2:48. §; az adott eseményhez kapcsolódó sajtó- és közfeladat-szabályok.

M-04 – Képviselő-testületi és bizottsági ülések nyilvánossága, közvetítése és felvételei

(1) A képviselő-testületi és bizottsági ülések nyilvánossága, zárt ülése, jegyzőkönyve, előterjesztése, hang- vagy videóközvetítése és felvétele külön adatkezelési célokat képezhet; ezek jogalapját és hozzáférési rendjét külön kell dokumentálni.

(2) A nyilvános ülés ténye nem jelenti, hogy minden elhangzó személyes adat korlátlanul, tartósan és kereshetően interneten közzétehető. A közzététel terjedelmét a jogszabályi nyilvánosság, az adattakarékosság és az érintetti jogok együttes figyelembevételével kell meghatározni.

(3) A közvetítés vagy felvételkészítés előtt a résztvevőket és felszólalókat egyértelműen tájékoztatni kell. Zárt ülés vagy zárt ülésre tartozó tartalom nem kerülhet nyilvános közvetítésbe vagy felvételbe.

(4) A honlapon közzétett jegyzőkönyveket, előterjesztéseket és felvételeket közzététel előtt adatvédelmi szempontból ellenőrizni, szükség szerint kitakarni, kivonatolni vagy hozzáférés-korlátozni kell.

Jogforrás / szakmai alap: Mötv. 46., 52. § és alkalmazandó ülésszabályok; GDPR 5–6., 12–14., 25. cikk; Infotv. közérdekű és közérdekből nyilvános adatokra vonatkozó rendelkezései.

M-05 – Beléptetési és vagyonvédelmi célú kamerás megfigyelés

(1) A modul kizárólag az Önkormányzat által adatkezelőként, beléptetési, vagyonvédelmi vagy személybiztonsági célból üzemeltetett, nem közterületi térfigyelő kamerás megfigyelésre alkalmazható. A közterületi térfigyelésre az M-06 modul és külön jogi vizsgálat irányadó.

(2) A kamerarendszer telepítése előtt dokumentálni kell a célt, jogalapot, szükségességet és arányosságot, kameránként a látómezőt, a maszkolást, a felvétel vagy élőkép használatát, a megőrzési időt, a hozzáférési kört és az adattovábbítási eseteket.

(3) Hangrögzítés csak külön, igazoltan szükséges és arányos jogalap alapján alkalmazható; alapértelmezett vagy kényelmi hangrögzítés tilos.

(4) A megfigyelt terület előtt rövid figyelemfelhívó jelzést, részletes tájékoztatót és érintetti kérelemkezelési eljárást kell biztosítani.

(5) A felvételek visszanézése, másolása, zárolása, átadása és törlése csak kijelölt személyek által, naplózott módon történhet. A megőrzési időt nem lehet általános „biztonsági" indokra hivatkozva korlátlanul meghatározni.

(6) A DPIA-kötelezettséget a GDPR 35. cikke és a NAIH listája alapján külön meg kell vizsgálni.

Jogforrás / szakmai alap: GDPR 5–6., 13., 21., 25., 32., 35. cikk; NAIH 35. cikk (4) szerinti lista; alkalmazandó vagyonvédelmi és munkajogi szabályok.

M-06 – Közterületi térfigyelő rendszer

(1) A rendszer működtetése előtt írásban azonosítani kell az adatkezelőt, az üzemeltetőt, a hozzáférésre jogosult személyeket, a feladat jogszabályi alapját, a megfigyelt közterületet, a célokat és az alkalmazandó adatvédelmi rezsimet.

(2) A GDPR és az Infotv. különös bűnüldözési szabályai nem keverhetők szabadon. A tájékoztatási, érintetti jogi, incidens- és nyilvántartási eljárást az alkalmazandó rezsim szerint kell kialakítani.

(3) Külön térfigyelő-kamerarendszer szabályzatot, kamerajegyzéket, térképet/látómező-leírást, hozzáférési és átadási naplót, megőrzési rendet és helyszíni tájékoztatást kell fenntartani.

(4) A felvételek felhasználása, hatóság részére átadása, kimentése és törlése kizárólag az alkalmazandó ágazati törvény és adatvédelmi szabályok szerint történhet.

(5) Az informatikai és fizikai védelmet, távoli hozzáférést, jogosultságokat, naplózást, mentést és incidenskezelést az IBSZ-ben és a kamerás szabályzatban összehangoltan kell szabályozni.

Jogforrás / szakmai alap: Az alkalmazandó rezsimtől függően GDPR vagy Infotv. 2. § (3) bekezdés és III/A. fejezet: a közterület-felügyeletről szóló 1999. évi LXIII. törvény és egyéb ágazati jogszabályok; NAIH vonatkozó tájékoztatói.

M-07 – Közvetlen önkormányzati jogviszonyok, pályáztatás és önkormányzati eszközhasználat

(1) A modul kizárólag az Önkormányzat mint önálló jogi személy saját, közvetlen foglalkoztatási, tisztségviselői, megbízási, pályázati, valamint az általa biztosított elektronikus levelezési és eszközhasználati adatkezeléseire alkalmazható. Nem terjed ki a polgármesteri vagy közös önkormányzati hivatal mint külön adatkezelő köztisztviselői, közszolgálati ügykezelői és munkavállalói adatkezelésére.

(2) A hivatal köztisztviselői és közszolgálati ügykezelői jogviszonyára a Kttv. vonatkozik. A közszolgálati alapnyilvántartásnál különösen a Kttv. 177. §-ában meghatározott zárt adatkört és a Kttv. 257. §-a szerinti jegyzői felelősséget kell figyelembe venni. E követelmények a hivatal később elkészítendő külön adatvédelmi és közszolgálati adatvédelmi szabályzatának tárgyát képezik.

(3) Az alkalmazandó foglalkoztatási szabályokat és a GDPR-jogalapot jogviszonyonként és adatkezelési célonként kell meghatározni. Jogszabályban előírt munkáltatói, közteherviselési, számviteli, közszolgálati vagy más kötelezettségnél főszabály szerint a GDPR 6. cikk (1) bekezdés c) pontja; közfeladat végrehajtásánál az e) pont; szerződéskötést megelőző vagy szerződéses adatkezelésnél a b) pont alkalmazhatóságát kell vizsgálni. Hozzájárulás csak ténylegesen önkéntes, elkülönült célra alkalmazható.

(4) A kiválasztási adatkezelés jogalapját a jogviszony típusához és pályázati eljáráshoz kell igazítani. A jelentkezés megküldése nem minősíthető automatikusan minden további célra adott hozzájárulásnak. Sikertelen pályázati anyag későbbi megőrzése csak külön jogalappal és megfelelő tájékoztatással történhet.

(5) Az önkormányzati elektronikus levelezés és eszközhasználat szabályozásában meg kell határozni a magánhasználat engedélyezését vagy tiltását, a naplózást, ellenőrzési célt, fokozatosságot, jogosultakat, érintetti jelenlétet, távolléti hozzáférést és jogviszony megszűnése utáni eljárást.

(6) A munkáltató nem jogosult korlátlanul bármely névre szóló e-mail tartalmába betekinteni. Az ellenőrzésnek célhoz kötöttnek, előre szabályozottnak, szükségesnek, arányosnak és lehetőség szerint fokozatosnak kell lennie.

(7) A postafiók megszűnés utáni kezelése során automatikus válasz, üzleti levelek átadása, hozzáférés-korlátozás, archiválás és törlési határidő alkalmazandó; a teljes postafiók határozatlan idejű megőrzése nem megengedett.

Jogforrás / szakmai alap: GDPR 5–6., 13., 21., 25., 32. cikk; Kttv. 1. § (1) bekezdés a)–b) pont, 177. §, 225/A–225/L. §, 257–258. § – kizárólag az adott jogviszony és szervezeti hatály szerint: Mt., Ptk. és az adott jogviszonyra vonatkozó ágazati szabályok; NAIH munkahelyi adatkezelési tájékoztatója (2016, a GDPR szerint aktualizálandó elvekkel).

M-09 – Hírlevél és lakossági kommunikáció

(1) A hírlevél vagy rendszeres elektronikus tájékoztatás címzettjeit, célját, jogalapját, feliratkozási és leiratkozási folyamatát külön kell meghatározni.

(2) Hozzájárulás alkalmazásakor a feliratkozás bizonyítékát, a tájékoztató verzióját és a hozzájárulás időpontját meg kell őrizni; a visszavonásnak egyszerűnek és díjmentesnek kell lennie.

(3) Közfeladati lakossági értesítés és marketingjellegű hírlevél nem kezelhető automatikusan azonos jogalapon. A címzettek láthatóságát tömeges e-mailnél technikailag meg kell akadályozni.

(4) Külső hírlevélszolgáltatónál adatfeldolgozói, adattovábbítási és biztonsági vizsgálat szükséges.

Jogforrás / szakmai alap: GDPR 5–7., 12–13., 21., 28., 44–49. cikk; elektronikus kereskedelmi és hírközlési szabályok az adott üzenettípus szerint.

M-10 – Pályázatok, támogatások, díjak és szerződéses partnerek közzététele

(1) Pályázati, támogatási, díjazási és szerződéses adatkezelésnél külön kell választani az ügyintézéshez szükséges belső adatkezelést, a jogszabályi adatszolgáltatást, a közérdekű adatigénylés teljesítését és a proaktív internetes közzétételt.

(2) Jogi személy szerződéses partner természetes személy kapcsolattartójának adatkezelése során a szükséges adatokat, jogalapot, tájékoztatást és megőrzést külön kell meghatározni.

(3) A közpénzek felhasználásával összefüggő közérdekből nyilvános adatok közzététele nem teszi automatikusan nyilvánossá a szükségtelen magánadatokat, aláírásképet, magánelérhetőséget vagy egyéb, a közzétételi célhoz nem szükséges személyes adatot.

(4) Az internetes közzététel előtt kitakarási és közzétételi ellenőrzőlistát kell alkalmazni; a közzétett dokumentumokat a közzétételi idő lejártakor felül kell vizsgálni vagy el kell távolítani.

Jogforrás / szakmai alap: GDPR 5–6., 13–14., 25. cikk; Infotv. közérdekű és közérdekből nyilvános adatokra, valamint elektronikus közzétételre vonatkozó rendelkezései; az adott támogatási vagy szerződéses ágazati jogszabály.