Terézváros

10/2021. (IX. 13.) számú polgármesteri-jegyzői közös utasítás

Budapest Főváros VI. kerület Terézváros Önkormányzata és Budapest Főváros VI. kerület Terézvárosi Polgármesteri Hivatal

Adatvédelmi és Adatbiztonsági Szabályzatáról

I. Fejezet
Általános rendelkezések

1. A szabályzat célja és hatálya

1. Az adatvédelmi és adatbiztonsági szabályzat (a továbbiakban: Szabályzat) célja, hogy a vonatkozó jogszabályok figyelembevételével meghatározza Budapest Főváros VI. kerület Terézváros Önkormányzata (a továbbiakban: Önkormányzat) és Budapest Főváros VI. kerület Terézvárosi Polgármesteri Hivatal (a továbbiakban: Hivatal) által nyilvántartott adatok kezelésének feltételeit, rendjét és az elektronikus ügyintézés során személyes adatokat tartalmazó adatállományok kezelését, biztosítva az adatvédelmi jogszabályok érvényesülését, megakadályozva az adatok titkosságának, sértetlenségének és rendelkezésre állásának elvesztését.

2. A Szabályzat hatálya kiterjed:
   a) az Önkormányzatnál és a Hivatalban foglalkoztatott valamennyi köztisztviselőre, közszolgálati ügykezelőre és munkavállalóra (a továbbiakban: foglalkoztatott),
   b) az Önkormányzat és a Hivatal teljeskörű feladat- és hatáskörének ellátására,
   c) az Önkormányzatnál és a Hivatalban nyilvántartott, valamint rendelkezésére álló személyes adatokra,
   d) az adatkezelés során felhasznált tárgyi, informatikai eszközökre, függetlenül annak üzemeltetési helyétől.

3. Az Önkormányzat és a Hivatal az általa kezelt személyes adatokat a kezelés teljes időtartama alatt szolgálati titoknak minősíti, az adatkezelést végző munkavállaló köteles e titkot megőrizni. A munkavállaló kötelessége továbbá, az általa kezelt adatok sértetlenségét biztosítani. Az Önkormányzat és a Hivatal kötelezettséget vállal arra, hogy az általa kezelt személyes adatokat kizárólag jelen szabályzatnak megfelelően az adatkezelési célok érdekében kezeli, azokat jogosulatlanul nem továbbítja, és nem hozza nyilvánosságra, továbbá a kezelt adatokat nem használja fel az adatkezelési céloktól eltérő célra. A titoktartási kötelezettség megszegése munkajogi, valamint büntetőjogi szankciót vonhat maga után.

2. Értelmező rendelkezések

4. A Szabályzat alkalmazása során használt fogalmakat az Európai Parlamentnek és a Tanácsnak a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet) szóló 2016. április 27-i (EU) 2016/679 rendeletével (a továbbiakban: GDPR) összhangban az alábbiak szerint kell értelmezni:

   a) *authentikáció:* hitelesítés, olyan folyamat, amely biztosítja és megerősíti a felhasználó azonosítását a rendszer számára.

b) *authorizáció:* engedélyezés, felhatalmazás. Olyan eljárás, amely megadott erőforrásokhoz (adatállományokhoz, valamilyen rendszer meghatározott szolgáltatásaihoz) való hozzáférést csak jogosultság esetén biztosít.
c) *titkosság:* az adat azon jellemzője, hogy csak a természetes személyek egy előre meghatározott köre (jogosultak) számára hozzáférhető, mindenki más számára hozzáférhetetlen.
d) *felfedés:* A titkosság elvesztése, amely esetén a titkos információ arra jogosulatlanok számára is ismertté, hozzáférhetővé válik.

5. A Szabályzatot az alábbi jogszabályokkal összhangban kell értelmezni és alkalmazni:
a) GDPR,
b) az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.),
c) az általános közigazgatási rendtartásról szóló 2016. évi CL. törvény (a továbbiakban: Ákr.),
d) a Polgári Törvénykönyvről szóló 2013. évi V. törvény (a továbbiakban: Ptk.),
e) az elektronikus ügyintézés és bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény (a továbbiakban: Eüsztv.),
f) az elektronikus ügyintézés részletszabályairól szóló 451/2016. (XII.19.) Korm. rend. (a továbbiakban: Eüszr.).

II. Fejezet
Általános adatkezelési szabályok

3. Az adatvédelem szervezete

6. A jegyző

a) elkészítteti az adatkezelési nyilvántartást és az adatvédelmi incidens nyilvántartást,
b) engedélyezi a nyilvántartási rendszerekhez a hozzáférési jogosultságot,
c) gondoskodik arról, hogy a főosztály- és osztályvezetők a munkafolyamatokat a beépített és alapértelmezett adatvédelemmel összhangban határozzák meg,
d) a tudomására jutott visszásság esetén utasítja az érintett foglalkoztatottat a jogszerűtlen adatkezelés megszüntetésére, szükség esetén fegyelmi eljárást kezdeményez a foglalkoztatottal szemben,
e) elkészítteti az adatvédelmi hatásvizsgálatot.

7. Az aljegyző

a) gondoskodik az adatkezelési nyilvántartást vezetéséről,
b) egyeztet az adatvédelmi incidensről az adatvédelmi tisztviselővel, gondoskodik az adatvédelmi incidens nyilvántartás vezetéséről és a természetes személyek jogaira és szabadságaira nézve kockázattal járó adatvédelmi incidenst bejelenti a Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: NAIH) részére,
c) szükség esetén gondoskodik az adatvédelmi ismeretek oktatásáról a foglalkoztatottak részére,

d) gondoskodik arról, hogy a főosztály- és osztályvezetők a munkafolyamatokat a beépített és alapértelmezett adatvédelemmel összhangban határozzák meg,
e) adatvédelmi szempontból véleményezi a képviselő-testületi és a bizottsági előterjesztéseket,
f) konkrét ügyekben felmerülő adatvédelmi kérdésekben segítséget nyújt a vezetők és az adatkezelők részére.

8. A főosztály- és osztályvezető

a) köteles az adatvédelemmel kapcsolatos jogszabályokat és a Szabályzatban foglaltakat megismerni, munkája során alkalmazni, valamint gondoskodni arról, hogy azt az osztályán dolgozó foglalkoztatottak megismerjék, előírásait munkavégzésük során alkalmazzák,
b) gondoskodik arról, hogy a munkafolyamatok meghatározása során a beépített és alapértelmezett adatvédelem követelményei megvalósuljanak,
c) konkrét ügyekben felmerülő adatvédelmi kérdésekben segítséget nyújt az általa irányított foglalkoztatottak részére,
d) jogszabályváltozás vagy más fontos okból javaslatot tesz a jegyzőnek a Szabályzat módosítására, kiegészítésére,
e) jogszabályváltozás esetén az adatkezeléseket áttekinti, és ha az adatkezelés módosul, megszűnik vagy új adatkezelés keletkezik vagy, ha egyébként indokoltnak tartja, javaslatot tesz az aljegyzőnek az adatkezelési nyilvántartás felülvizsgálatára és módosítására,
f) a hozzá érkező adatkezeléssel kapcsolatos panaszokat az adatvédelmi tisztviselő bevonásával kivizsgálja, az érintett részére választ készít elő az adatvédelmi tisztviselő bevonásával, melyet továbbít a jegyző részére,
g) a tudomására jutott visszásságról, adatvédelmi incidensről tájékoztatja a jegyzőt.

9. Az adatkezelést végző foglalkoztatott

a) köteles az adatvédelemmel kapcsolatos jogszabályokat és a Szabályzatot megismerni és maradéktalanul betartani,
b) köteles tájékoztatni közvetlen felettesét a feladatkörében felmerült adatvédelmi incidensről, bármely adatvédelmi problémáról, észrevételeiről, a számítástechnikai eszközök bárminemű meghibásodásáról, az adatállomány kezelhetőségében bekövetkezett problémáról,
c) köteles a tudomására jutott, az adatkezeléssel kapcsolatosan feltárt visszásságot haladéktalanul megszüntetni,
d) gondoskodik arról, hogy az általa kezelt adatokhoz jogosulatlanul ne férhessen hozzá harmadik személy, ügyel a személyes adatokat tartalmazó iratok, dokumentumok, nyilvántartások biztonságos tárolására,
e) a jogszabály által felhatalmazott személynek vagy szervezetnek adatot szolgáltat, adatot továbbít,
f) köteles közvetlen felettesét, szükség esetén az aljegyzőt tájékoztatni minden olyan eseményről, amikor őt jogszerűtlen adatkezelésre kérték fel, utasították,
g) haladéktalanul jelzi közvetlen felettesének, ha az adatállományba jogosulatlan hozzáférést vagy bárminemű változást tapasztal,
h) fegyelmi és kártérítési felelősséggel tartozik azért, hogy tevékenységét az adatkezelésre és az adatok védelemére vonatkozó jogszabályoknak, valamint a

Szabályzatnak, az adatkezelést elrendelő jogszabály hiányában pedig az érintett hozzájárulásának megfelelően végezze.

10. Az adatvédelmi tisztviselő

a) tájékoztat és szakmai tanácsot ad az adatkezelő vagy az adatfeldolgozó, továbbá az adatkezelést végző alkalmazottak részére adatvédelmi kérdésben,
b) az adatkezelési nyilvántartást felveszi és közreműködik a nyilvántartás aktualizálásában,
c) adatvédelmi incidens nyilvántartás mintát elkészíti és közreműködik a vezetésében,
d) részt vesz az adatvédelmi incidensek kivizsgálásában, ennek során együttműködik az információbiztonsági felelőssel,
e) ellenőrzi a GDPR-nak, valamint az Info tv-nek, továbbá a személyes adatok védelmével kapcsolatos belső szabályoknak való megfelelést, ideértve a feladatkörök kijelölését, az adatkezelési műveletekben részt vevő személyzet tudatosság-növelését és képzését, valamint a kapcsolódó auditokat is,
f) javaslatot tesz érdekmérlegelési teszt, valamint adatvédelmi hatásvizsgálat elvégzésére, kérésre szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, valamint nyomon követi a hatásvizsgálat elvégzését,
g) együttműködik a NAIH-hal, és az adatkezeléssel összefüggő ügyekben - ideértve az előzetes konzultációt is - kapcsolattartó pontként szolgál a NAIH felé, valamint adott esetben bármely egyéb kérdésben konzultációt folytat vele,
h) adattudatosság növelése érdekében évente kétszer adatvédelmi oktatást tart.

11. Az informatikus

a) gondoskodik az elektronikus információs rendszerek logikai védelméről,
b) gondoskodik az elektronikusan kezelt személyes adatok biztonsági mentéséről, azok biztonságos tárolásáról, archiválásáról, adatkezelési idő lejártát követő törléséről,
c) együttműködik az adatvédelmi hatásvizsgálat elkészítésében, az adatvédelmi incidens kivizsgálásában,
d) elektronikus adatkezelések esetében kérésre javaslatot ad olyan informatikai, műszaki megoldásokra, mellyel a megfelelő adatvédelmi és adatbiztonsági szint biztosítható.

4. Az adatkezelések jogalapja

12. A Hivatal és az Önkormányzat elsődlegesen közfeladatellátása során kezel személyes adatokat. A személyes adatok kezelése közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükségesek [GDPR 6. cikk (1) bekezdés e) pont].

13. A 12. ponttól eltérően

a) a Hivatal és az Önkormányzat saját vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges mértékben
aa) személy- és vagyonbiztonság védelme céljából a Rendészeti Osztályon az ügyféltérben, valamint jelentős értékű vagyontárgyak védelmére és a szerverterem figyelésére, továbbá a Hivatal épületében a szerverterem vagyonvédelme céljából kamerás adatkezelést végez,
ab) beléptető rendszert működtet,

b) tájékoztatáson alapuló, az érintett kifejezett, egyértelmű és önkéntes hozzájárulásán alapuló adatkezelést is végez.

14. A Hivatal és az Önkormányzat az adatkezelés megkezdését megelőzően az adatkezelés jogalapját megvizsgálja.

5.Adatkérés, adatbefogadás szabályai hozzájáruláson alapuló adatkezelési tevékenység esetén

15. Ha az adatkezelés jogalapja az érintett tájékoztatáson alapuló önkéntes és egyértelmű hozzájárulása, abban az esetben csak az adatkezelési hozzájárulás megadása esetén végezhető adatkezelési tevékenység.

16. A hozzájárulás megadásának megtagadása esetén adatkezelés nem végezhető.

17. Az adatot fogadó foglalkoztatott a hozzájáruló nyilatkozatot tartalmazó nyomtatvány eredeti példányát az Iratkezelési szabályzatban meghatározott előírások szerint köteles kezelni.

18. Amennyiben az érintett utóbb visszavonja az adatkezelési hozzájárulását, a személyes adatok tovább nem kezelhetőek. A hozzájárulás visszavonása a visszavonást megelőző adatkezelés jogszerűségét nem érinti.

19. Az adatkezelés során - függetlenül attól, hogy papír alapon vagy elektronikus adatfeldolgozó rendszeren történt-e az adat fogadása - biztosítani kell, hogy a nyomtatványon rögzített adatokon túlmenően az adatbefogadás időpontja, valamint az adatkezelést végző alkalmazott azonosítója visszakereshető módon tárolásra kerüljön.

6.Az érintetti jogok gyakorlása

6.1. Tájékoztatási kötelezettség és az érintett hozzáférési joga

20. Az adatkezeléshez használt papír és elektronikus nyomtatványokon az érintett személyes adatainak kezelésére vonatkozó tájékoztatás elhelyezésre kell, hogy kerüljön. Az érintettnek a nyomtatvány aláírásával, illetve elektronikus továbbítását megelőzően egyértelműen nyilatkozni kell, hogy az adatkezelési tájékoztató tartalmát megértette-e. Ha az adatkezeléshez az érintett hozzájárulása is szükséges, akkor az adatkezelési tájékoztatást követően nyilatkoztatni szükséges arról, hogy megadja-e a hozzájárulását a nyomtatványon rögzített személyes adatainak kezeléséhez.

21. Az adatkezelési tájékoztatás az Önkormányzat honlapján is elhelyezhető. Ebben az esetben a nyomtatványon utalni kell a pontos URL megjelölésével az adatkezelési tájékoztató elérhetőségi helyére.

22. Az érintett személyesen vagy hivatali kapun is kérhet tájékoztatást a vele kapcsolatban kezelt adatokról.

23. A tájékoztatás minden esetben tartalmazza a GDPR-ban előírtakat.

24. Az érintett a saját személyes adataival kapcsolatos adatkezelésbe oly módon tekinthet be, hogy más érintett személyes adatairól, azok kezeléséről semmilyen információt sem nyerhet.

25. Abban az esetben, ha az érintett részletes tájékoztatást kér a 3. személy felé történt adattovábbításról vagy az adatok nyilvánosságra hozataláról, akkor a tájékoztatást végző foglalkoztatott kötelessége az ügyfelet az érintett adatkezelést végző szervezeti egységhez irányítani, aki köteles a szükséges tájékoztatási és betekintési kötelezettségnek eleget tenni. A tájékoztatást írásban 1 hónapon belül kell elvégezni.

26. Az adatkezelést végző szervezeti egység a betekintési kötelezettséget csak akkor tagadhatja meg, ha a kért adatokat az illetékes szerv a megfelelő eljárás keretében – a minősített adatok védelméről szóló 2009. évi CLV. törvény szabályai szerint – előzetesen minősített adattá nyilvánította, mely esetben az adatkezelést végző szervezeti egység köteles az érintettel a közlés megtagadásának indokát közölni.

27. Az adatkezelést végző szervezeti egység az érintett kérésére az adatkezelés tárgyát képező személyes adatok másolatát az érintett rendelkezésére bocsátja.

28. Az érintett által kért további másolatokért az adatkezelő az adminisztratív költségeken alapuló alábbi észszerű mértékű díjat számolja fel:

    a) fénymásolás költsége,
    b) adathordozó költsége.

    A megállapított költséget a Hivatal házi pénztárába kell befizetni vagy a Hivatal 11784009-15735698 számú számlájára utalással kell teljesíteni.

6.2. Az érintett tiltakozása

29. Az érintett adatkezelés elleni tiltakozását írásban vagy elektronikus úton az alábbi címen teheti meg:

    Budapest Főváros VI. kerület Terézváros Jegyzője
    1067 Budapest Eötvös u. 3.
    jegyzo@terezvaros.hu

30. Az érintett tiltakozási kérelmét a jegyző köteles a tiltakozás benyújtását követő 1 hónapon belül kivizsgálni, az adatkezelést végző szervezeti egységnél a szükséges vizsgálatot, ellenőrzést lefolytatni és a vizsgálat eredményéről az érintettet tájékoztatni.

6.3. A helyesbítéshez való jog

31. Az Önkormányzat és a Hivatal minden észszerű intézkedést megtesz annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul helyesbítsék.

32. Figyelembe véve az adatkezelés célját, az érintett jogosult arra, hogy kérje a hiányos, pontatlan személyes adatok - kiegészítő nyilatkozat útján történő – kiegészítését, javítását az alábbi elérhetőségen:

Budapest Főváros VI. kerület Terézváros Jegyzője
1067 Budapest Eötvös u. 3.
jegyzo@terezvaros.hu

33. A helyesbítésről azt a címzettet, akivel a személyes adatot korábban közölték – kivéve, ha ez lehetetlen vagy aránytalanul nagy erőfeszítést jelent – tájékoztatni köteles a jegyző.

6.4. Adatok törlése, elfeledtetéshez való jog

34. Az adatok megőrzési ideje adatkezelésenként kerül meghatározásra a mindenkor hatályos önkormányzati irattári terv alapján.

35. Az Önkormányzat és a Hivatal az érintett számára biztosítja a lehetőséget, hogy az érintett megkeresésére az adatokat törli a GDPR-ban meghatározott esetekben.

36. Az Önkormányzat és a Hivatal azonnal végrehajtja az általa kezelt adatok törlését, ha annak végrehajtását jogerős bírósági ítélet rendeli el, vagy a NAIH az adatkezelés jogellenességét megállapítja, elrendeli az adatok törlését és az Önkormányzat vagy Hivatal e döntés ellen bírósághoz nem fordul.

37. Az Önkormányzat és a Hivatal a papír alapú adathordozókon tárolt adatok törlését

a) az Iratkezelési szabályzat selejtezési előírásai szerint, jelen szabályzat adatbiztonsági előírásait figyelembe véve hajtja végre. Az adat törlését minden esetben az adatkezelésért felelős szervezeti egység vezetője köteles kezdeményezni, a selejtezésről jegyzőkönyvet kell készíteni.
b) amennyiben az irat nem selejtezhető, akkor a személyes adatnak az iratból történő törlésével (anonimizálással) kell végrehajtani.

38. Az adatok törlését az adatkezelést végző szervezeti egység vezetője utasítására a kijelölt alkalmazott hajtja végre.

39. A törlésről azt a címzettet, akivel a személyes adatot közölték – kivéve, ha ez lehetetlen vagy aránytalanul nagy erőfeszítést jelent – tájékoztatni köteles a jegyző.

6.5. Adatkezelés korlátozásához való jog

40. Az érintett a jegyzőhöz címzett kérelemmel a foglalkoztatottól vagy az adatkezelést végző szervezeti egységtől kérheti a személyes adatai kezelésének a korlátozását.

41. Az érintett a tiltakozást az alábbi elérhetőségen teheti meg:

Budapest Főváros VI. kerület Terézváros Jegyzője
1067 Budapest Eötvös u. 3.
jegyzo@terezvaros.hu

42. A jegyző köteles a korlátozási igényt 1 hónapon belül megvizsgálni és a vizsgálat eredményéről az érintettet, valamint azt a címzettet, akivel a személyes adatot közölték – kivéve, ha ez lehetetlen vagy aránytalanul nagy erőfeszítést jelent - tájékoztatni.

6.6. Adathordozhatósághoz való jog

43. Az érintett az ügyfélszolgálaton vagy az adatkezelést végző szervezeti egységtől kérheti, hogy a rá vonatkozó, általa egy adatkezelő rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja, továbbá azt, hogy ezeket az adatokat egy másik adatkezelőnek továbbítsa.

44. Az érintett a kérelmét írásban az alábbi címen nyújthatja be:

Budapest Főváros VI. kerület Terézváros Jegyzője
1067 Budapest Eötvös u. 3.
jegyzo@terezvaros.hu

45. Az adatok előállításában az Informatikai Csoport közreműködik, amennyiben a szervezeti egység nem tudja előállítani tagolt, széles körben használt, géppel olvasható formátumban.

7. Adatok tárolása, archiválása

46. A személyes adatok biztonságos tárolását papír alapú adatkezelés és feldolgozás esetén az Iratkezelési szabályzat és jelen szabályzat adatbiztonságra vonatkozó rendelkezései biztosítják.

8. Adatok másolása, adatkezelések összekapcsolása

47. Az érintett adatok másolása, azokból származtatott – de a személy azonosítására alkalmas – új adatok létrehozása, más adatbázisokkal összekapcsolása új adatkezelésnek minősül, melyhez az Önkormányzatnak vagy a Hivatalnak GDPR-ban rögzített jogalappal kell rendelkeznie.

48. Az adatokból képzett, a személy azonosítására alkalmas adatoktól megfosztott újonnan képzett adatokat, melyekből az érintetthez köthető személyes adat már semmilyen módon nem állítható helyre, az Önkormányzat vagy a Hivatal felhasználhatja statisztikák, belső kimutatások készítésére.

9. Adattovábbítás

49. Megkeresésre akkor lehet adatot továbbítani, ha a megkeresést küldő megindokolta, a GDPR-ban rögzített valamely jogalappal, jogszabályi hivatkozással alátámasztotta a személyes adat kezelésére való jogosultságát.

50. Személyes adat telefonon, telefaxon nem továbbítható.

51. Személyes adat e-mailen jelszóval védett fájlban továbbítható kizárólag. A jelszó nem küldhető ugyanazon a csatornán át, mint, amin a jelszóval védett fájl kerül továbbításra.

52. Az adatkezelő az adattovábbítás jogszerűségének ellenőrzése, valamint az érintett tájékoztatása céljából adattovábbítási nyilvántartást vezet, amely tartalmazza az általa kezelt személyes adatok továbbításának időpontját, az adattovábbítás jogalapját és címzettjét, a továbbított személyes adatok körének meghatározását, valamint az adatkezelést előíró jogszabályban meghatározott egyéb adatokat.

53. Annak érdekében, hogy az érintett adataival kapcsolatos információs önrendelkezési jogát megfelelően gyakorolhassa, az Önkormányzat és a Hivatal automatizált munkafolyamataiban olyan naplózási rendszert használ, amely lehetővé teszi, hogy az érintett adatainak harmadik személy felé történő adattovábbítása, beleértve a továbbítás időpontját, a pontos adattartalmat, visszakereshetővé váljon.

10. Nyilvánosságra hozatal

54. Az Önkormányzat és a Hivatal személyes adatot kizárólag akkor hozhat nyilvánosságra, ha arra a GDPR-ban szabályozott jogalappal rendelkezik.

55. Személyes adatokat tartalmazó iratok kizárólag anonimizált módon, a statisztikai adatok szabadon hozhatók nyilvánosságra.

III. Fejezet
Elektronikus ügyintézésre vonatkozó speciális adatkezelési rendelkezések

11. Az elektronikus ügyintézés során történő adatkezelés célja

56. Az elektronikus ügyintézés keretében kezelt személyes adatok kezelésének a célja annak biztosítása, hogy az Önkormányzat és a Hivatal az általa végzett elektronikus ügyintézés során megfeleljen a GDPR, az Infotv., az Ákr., az Etv. és az elektronikus ügyintézés részletszabályairól szóló 451/2016. (XII.19.) Korm. rendelet szabályainak és a kapcsolódó jogszabályoknak, továbbá az önkormányzat által az ügyfélkapcsolat során kezelt személyes adatok kezelésének elsődleges célja az ügyfél és az önkormányzat között létrejött hatósági ügyfélkapcsolat szabályozása, beleértve

a) az elektronikus úton történő regisztrációt,
b) a személyes jelenlét mellett végzett azonosítást és
c) az ügyfél és az Önkormányzat, valamint a Hivatal között hatósági ügyfélkapcsolat során végzett elektronikus ügyintézést.

12. Kezelt személyes adatok forrása

57. Az Önkormányzat és a Hivatal az elektronikus ügyintézéshez az alábbi módon gyűjt elektronikusan személyes adatokat:

a) regisztráló ügyfelektől,
b) személyesen azonosított ügyfelektől,

c) elektronikus ügyintézés során eredményes kérelmet benyújtott ügyfelektől,
d) elektronikus ügyintézés során elutasított kérelmet benyújtott ügyfelektől,
e) közhiteles és nem közhiteles nyilvántartásból.

58. Az érintettek az elektronikus ügyintézésre történő regisztráció során elektronikus nyomtatványt töltenek ki. Az elektronikus nyomtatvány fogadása esetén az elfogadás feltétele, hogy az alábbi adatok rendelkezésre álljanak:

a) a küldő munkaállomás IP címe és
b) a küldés időpontja.

13. A regisztráló ügyfeleket érintő adatkezelés

59. Az Önkormányzat és a Hivatal azon személyes adatokat kezeli, amelyeket az ügyfél az elektronikus ügyintézésre történő elektronikus regisztráció (a továbbiakban: előregisztráció) során megad.

60. Az adatok forrása az érintett által benyújtott és az ügyfélszolgálaton érkeztetett, kitöltött elektronikus formanyomtatvány.

61. Az adatkezelésre az Önkormányzat és a Hivatal jogosult.

62. A személyes adatok kezelését megelőzően az adatkezelő tájékoztatást ad az adatkezelésről a GDPR előírásai szerint.

63. A jegyző gondoskodik arról, hogy az elektronikus regisztráció során felhasznált formanyomtatványon rögzítve legyen minden információ, melyek a teljeskörű adatvédelmi tájékoztatáshoz szükségesek.

64. Az adatkezelés célja az ügyfelek regisztrálása a hivatali ügyintézés egyszerűsítése, meggyorsítása érdekében.

65. Az adatkezelés jogalapja a GDPR 6. cikk (1) bekezdés e) pontja, mivel az Önkormányzat és a Hivatal közfeladat ellátásához szükséges a személyes adatok kezelése.

66. Az ügyfelek részére az előregisztrálással felhasználói fiók jön létre.

67. Az Önkormányzat és a Hivatal az ügyfél által az előregisztráció során kitöltött formanyomtatványt elektronikus úton fogadja be.

68. Az adatváltoztatási kérelmet új formanyomtatvány benyújtásával lehet kezdeményezni, melynek kezelési szabályai azonosak az új adatok fogadásának szabályaival.

69. A személyes adatok elektronikus feldolgozása, tárolása az E-ügyintézés rendszerben történik.

70. Az adatkezelő az elektronikus ügyintézési felület üzemeltetésére adatfeldolgozót vesz igénybe.

71. Az adatok másolása, adatkezelések összekapcsolása tilos.

72. Az adatokat törölni a jogszabályban és irattári tervben előírt iratmegőrzési kötelezettség időtartama alatt tilos.
Ez alól kivételt képez, ha
a) az érintett tiltakozott az adattkezelés ellen és az adatkezelő, a NAIH vagy a bíróság helyt adott a kérelemnek vagy
b) a 84. pont szerinti esteben (az érintett a személyes adatainak megfelelőségét hitelt érdemlő módon nem igazolja, vagy az egyeztetés során felmerült eltérések pontosításában nem közreműködik).

14. Személyesen azonosított ügyfélkapuval nem rendelkező ügyfelek adatai

73. Az Önkormányzat és a Hivatal az ügyfélkapuval nem rendelkező ügyfél által az elektronikus ügyintézésre történő előregisztráció során megadott személyes adatokat a személyazonosító okmányok adataival egybeveti és a személyes adatok azonosságát ellenőrzi az érintett személyes megjelenése során. A formanyomtatvány az érintett aláírásával ellátva fogadható be. A regisztráció a személyazonosság igazolásával zárul le.

74. Az adatok felett adatkezelői feladatot az Önkormányzat és a Hivatal lát el.

75. A személyes adatok kezelését megelőzően az adatkezelő tájékoztatást ad az adatkezelésről a GDPR előírásai szerint.

76. A jegyző gondoskodik arról, hogy a nyomtatvány tartalmazzon minden információt, melyek a személyes azonosításhoz és a teljeskörű adatvédelmi tájékoztatáshoz szükségesek.

77. Az adatkezelés célja, hogy az Önkormányzat és a Hivatal egyeztesse az előregisztráció során az elektronikus felületen kitöltött formanyomtatványban szereplő adatok azonosságát az ügyfél személyazonosító okmányaival és a személyes adatokat az elektronikus ügyintézés céljából összegyűjtse, rögzítse, ellenőrizze és tárolja.

78. Az adatkezelés jogalapja a GDPR 6. cikk (1) bekezdés e) pontja, mivel az Önkormányzat és a Hivatal közfeladat ellátásához szükséges a személyes adatok kezelése.

79. Az adatok forrása az érintett által az ügyfélszolgálaton érkeztetett, kitöltött elektronikus előregisztrációs formanyomtatvány, az ügyfél által a személyes megjelenés során kitöltött nyilatkozat, valamint az ügyfélszolgálat előtt személyesen megjelent ügyfél által bemutatott személyi azonosító okmányok.

80. A személyes adatok elektronikus feldolgozása, tárolása az E-ügyintézés rendszerben történik.

81. Az adatkezelő az elektronikus ügyintézési felület üzemeltetésére adatfeldolgozót vesz igénybe.

82. Az adatváltoztatási kérelmet új formanyomtatvány benyújtásával lehet kezdeményezni, melynek kezelési szabályai azonosak az új adatok fogadásának szabályaival.

83. Az adatok másolása, adatkezelések összekapcsolása tilos.

84. Amennyiben az ügyfél a személyes regisztráció során adatkezelési tájékoztatást követően a személyes adatainak megfelelőségét hitelt érdemlő módon nem igazolja, vagy az egyeztetés során felmerült eltérések pontosításában nem közreműködik, az adatkezelő az adatokat törli. Minden egyéb esetben az Önkormányzat vagy Hivatal az adatokat addig az időpontig tárolja, ameddig a jogszabályokban rögzített kötelezettség teljesítése szempontjából szükséges.

15. Az elektronikus ügyintézés során szabályos kérelmet benyújtott ügyfelek adatai

85. Az Önkormányzat és a Hivatal az ügyfél által közfeladat ellátáshoz elektronikus regisztráció során megadott személyes adatokat kezeli.

86. Az adatok feletti adatkezelői feladatokat az Önkormányzat és a Hivatal látja el.

87. Az adatkezelő az adatkezelést megelőzően tájékoztatást ad az adatkezelésről a GDPR előírásai szerint.

88. A jegyző gondoskodik arról, hogy a kérelem nyomtatványon rögzítésre kerüljön a GDPR szerinti részletezettséggel az adatkezelési tájékoztatás.

89. Az adatkezelés célja a hatósági ügyintézés során az ügyfél által benyújtott kérelem elbírálása és a kérelem alapján az Önkormányzat vagy a Hivatal döntésének meghozatala.

90. Az adatkezelés jogalapja a GDPR 6. cikk (1) bekezdés e) pontja, mivel az Önkormányzat és a Hivatal közfeladat ellátásához szükséges a személyes adatok kezelése.

91. Az adatok forrása az érintett által az előregisztráció során kitöltött, az ügyfélszolgálaton érkeztetett elektronikus formanyomtatvány, az ügyfél által a regisztráció során kitöltött nyilatkozat, az ügyfélszolgálat előtt személyesen megjelent ügyfél által bemutatott személyazonosító okmányok, valamint az Önkormányzat és a Hivatal által teljesített adattovábbítást követően a Belügyminisztériumtól az Önkormányzathoz vagy a Hivatalhoz visszaérkezett adatok.

92. Az Önkormányzat és a Hivatal a regisztrációs kérelem elfogadásához, továbbá az engedély megadása érdekében adategyeztetés céljából az adatkezelést összekapcsolhatja a Belügyminisztérium nyilvántartásával személyes adatok ellenőrzése céljából.

93. Az adatkezelő az érintett személyes adatainak ellenőrzését követően, az érintett aláírásával ellátott elektronikus nyomtatványt a Belügyminisztérium számára automatikusan elektronikusan továbbítja, az adatkérésre válaszként érkezett adatokat elektronikus úton fogadja be.

94. A személyes adatok elektronikus feldolgozása, tárolása az E-ügyintézés rendszerben történik.

95. Az adatkezelő az elektronikus ügyintézési felület üzemeltetésére adatfeldolgozót vesz igénybe.

96. Az adatváltoztatási kérelmet új formanyomtatvány benyújtásával lehet kezdeményezni, melynek kezelési szabályai azonosak az új adatok fogadásának szabályaival.

97. Az Önkormányzat és a Hivatal a hatósági ügyintézéssel kapcsolatban keletkezett iratokat a hatályos jogszabályokban meghatározott ideig őrzi, azokat a köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről szóló 1995. évi LXVI. törvény és a közfeladatot ellátó szervek iratkezelésének általános követelményeiről szóló 335/2005. (XII. 29.) Korm. rendelet szerint kezeli.

16. Közhiteles és nem közhiteles adatbázisból lekért adatok

98. Az Önkormányzat és a Hivatal a hatósági ügyintézés során a kérelem elbírálásához szükséges adatokat közhiteles és nem közhiteles nyilvántartásokból lekérdezi és azokat az ügyintézés során felhasználja és tárolja.

17. Önkormányzati, hivatali megkeresésekhez hozzájárult ügyfelek nyilvántartása

99. Az Önkormányzat és a Hivatal elektronikus úton és hagyományos úton küldött levelek, telefonhívások, illetve közvetlen személyes megkeresés útján az érintett hozzájárulásával

a) részére tájékoztatást nyújt az Önkormányzat és a Hivatal működésével kapcsolatos aktuális kérdésekről, döntésekről,
b) az Önkormányzat és a Hivatal tevékenységével kapcsolatos elégedettségét felméri, valamint minőségbiztosítási okokból adatokat gyűjt.

100. Az adatkezelői feladatokat az Önkormányzat és a Hivatal látja el.

101. Az adatkezelő adatkezelésének jogalapját az ügyfél előzetes tájékoztatáson alapuló önkéntes és egyértelmű hozzájárulása adja.

102. A jegyző gondoskodik arról, hogy a használt webes felületen és formanyomtatványon az adatkezelési hozzájárulás megadását megelőzően elérhető legyen a GDPR-ban előírt részletezettségű adatkezelési tájékoztatás.

103. Az adatok forrása az érintett által az ügyfélszolgálaton érkeztetett, kitöltött elektronikus formanyomtatvány, az ügyfél által a regisztráció során kitöltött nyomtatvány, valamint az ügyfélszolgálat előtt személyesen megjelent ügyfél által bemutatott személyi azonosító okmányok.

104. Az adatkezelő a személyes adatokat az elektronikus felületen végzett regisztráció vagy személyes megjelenés során az érintett által megadott személyes adatok rögzítése során fogadja be.

105. A személyes adatok feldolgozása és tárolása elektronikus adatfeldolgozó rendszerrel az E-ügyintézési rendszer adatállományában történik.

106. Az adatkezelő az elektronikus ügyintézési felület üzemeltetésére adatfeldolgozót vesz igénybe.

107. Az adatváltoztatási kérelmet új formanyomtatvány benyújtásával lehet kezdeményezni, melynek kezelési szabályai azonosak az új adatok fogadásának szabályaival.

108. Az Önkormányzat és a Hivatal az adatokat kizárólag az adatkezelési cél érdekében tárolhatja, az adatbázis más adatbázisokkal való összekapcsolására nem kerülhet sor.

109. Az Önkormányzat és a Hivatal az adatkezelési céllal kapcsolatban keletkezett iratokat az adatkezelési céllal összhangban meghatározott ideig őrzi, azokat a köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről szóló 1995. évi LXVI. törvény és a közfeladatot ellátó szervek iratkezelésének általános követelményeiről szóló 335/2005. (XII. 29.) Korm. rendelet szerint kezeli.

110. A személyes adatokat haladéktalanul, de legkésőbb 3 munkanapon belül törölni kell, ha az érintett utóbb visszavonja az adatkezelési hozzájárulását. A hozzájárulás visszavonása a visszavonást megelőző adatkezelés jogszerűségét nem érinti.

IV. Fejezet
Adatkezelő adatvédelemmel kapcsolatos egyéb feladatai

18. Az adatkezelési tevékenységek nyilvántartása

111. Az adatkezelési tevékenységek nyilvántartását az aljegyző vezeti.

112. Minden új adatkezelési tevékenység bevezetése előtt az adatkezelésért felelős szervezeti egység vezetője köteles az adatkezelést jelezni az aljegyzőnek. Az új adatkezelést az adatkezelési tevékenységek nyilvántartásába fel kell venni.

113. Az adatkezelési tevékenység módosulása esetén az adatkezelést végző szervezeti egység vezetője köteles a módosulást jelezni az aljegyző számára. A változást az adatkezelési tevékenységek nyilvántartásán át kell vezetni.

114. Az adatvédelmi tisztviselő köteles együttműködni az adatkezelési nyilvántartás felvétele, kiegészítése és módosítása során.

19. Adatvédelmi incidens

115. Amennyiben a foglalkoztatott a biztonság olyan sérülését észleli, amely a kezelt - továbbított, tárolt vagy más módon kezelt - személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi vagy eredményezte, az észlelést követően haladéktalanul köteles jelezni ezt a vezetője részére. A vezető az incidensről értesíti a jegyzőt.

116. A jegyző az adatvédelmi incidens kivizsgálásáról haladéktalanul intézkedik az aljegyző, az érintett szervezeti egység, az Informatikai Csoport, az adatvédelmi tisztviselő és az információbiztonsági felelős bevonásával.

117. Amennyiben valószínűsíthető, hogy személyes adatokat nagy számban érint vagy különleges személyes adatokat érint, vagy más egyéb módon természetes személyek jogaira és szabadságaira nézve kockázattal jár az incidens, akkor az aljegyző gondoskodik az adatvédelmi incidensnek a NAIH részére történő haladéktalan, legkésőbb 72 órán belül történő bejelentéséről, valamint az érintettek értesítéséről a GDPR-ban előírtak szerint.

118. Az incidensről jegyzőkönyvet kell felvenni, amiben dokumentálni kell legalább:

a) az esemény leírását, érintettek körét, számát, a valószínűsíthetően bekövetkező kár ismertetését,
b) a bekövetkezett károk elhárítása, a jogosulatlan adatkezelés megszüntetése, adatok helyreállítása, adatok hozzáférhetetlenné tétele érdekében megtett intézkedéseket és
c) azon intézkedéseket, amelyek jövőbeli incidens elkerülését célozzák.

119. Az adatvédelmi incidens bekövetkezését követően legalább az érintett szervezeti egység foglalkoztatottai részére soron kívüli adatvédelmi oktatást kell tartani.

120. Az 1. melléklet szerinti adatvédelmi incidens nyilvántartását az aljegyző vezeti.

20. Adatvédelmi hatásvizsgálat

121. Amennyiben a Hivatal vagy az Önkormányzat a GDPR 35. cikk (1) és (3) bekezdésében nevesített vagy a NAIH honlapján közzétett adatvédelmi hatásvizsgálat köteles adatkezeléseket végez, akkor a szervezeti egység vezetője erről tájékoztatja az aljegyzőt, aki gondoskodik az adatvédelmi hatásvizsgálat elvégzéséről.

122. A NAIH által közzétett listában szereplő adatkezelési műveleteken túl is kötelessége a Hivatalnak és az Önkormányzatnak az általa folytatott adatkezelések vonatkozásában az adatvédelmi kockázatok felmérése és a megfelelő kockázatkezelés.

123. Az adatvédelmi hatásvizsgálat elvégzésébe be kell vonni legalább

a) az adatkezelést végző szervezeti egységet,
b) az adatvédelmi tisztviselőt,
c) adatbiztonsági kérdésekben, különösen az adatok logikai védelmét érintően az Informatikai Csoportot és az információbiztonsági felelőst.

124. Ha a Hivatal és az Önkormányzat nem tudja a kockázatokat az elfogadható szintre csökkenteni, akkor a jegyző előzetes konzultációt kezdeményez a NAIH-hal.

125. Az adatvédelmi hatásvizsgálatot az aljegyző tartja nyilván.

V. Fejezet
Biztonsági követelmények

21. Az adatok fizikai védelme

126. Azokban a helyiségekben, amelyekben személyes adatok kezelése történik, csak az alábbi személyek tartózkodhatnak:
a) munkavégzés céljából jelen lévő foglalkoztatott,

b) az érintett vagy törvényes képviselője, valamint az érintett által felhatalmazott személy.

127. A foglalkoztatott a nála lévő iratokat köteles munkaidőn túl – és amelyeket lehetséges, munkaidőben is – szekrényben tartani. Az asztalon, az irodában, illetve egyéb harmadik személy számára is hozzáférhető helyen hivatalos iratok csak munkavégzés céljából és annak tartama alatt tárolhatók.

128. Személyes adatokat is tartalmazó iratot a Hivatalból kivinni, munkahelyen kívül tanulmányozni, feldolgozni, tárolni kizárólag munkaköri feladat ellátásával kapcsolatban és kizárólag a jegyző engedélyével lehet. A foglalkoztatott ez esetben is köteles gondoskodni arról, hogy az irat ne vesszen el, ne rongálódjon, vagy ne semmisüljön meg, és tartalma ne jusson illetéktelen személy vagy szerv tudomására.

129. Az iratról másolat készítését oly mértékben kell biztosítani, hogy az harmadik személy személyes adatait ne tartalmazza, illetve az harmadik személy személyiségi jogait ne sértse.

22. A manuálisan kezelt adatok fizikai védelme

130. A manuálisan kezelt személyes adatokat keletkezésükkor megfelelő minőségű (hagyományos papír, formanyomtatvány) adathordozóra kell rögzíteni.

131. Az adatok olvashatóságáért az azokat felvevő, illetve rögzítő (leíró) foglalkoztatott felel.

132. Az adatokat rendezett, visszakereshető formában, zárható irodában, illetve megfelelő helyen kell tárolni.

133. A nagy mennyiségű adat tárolására szolgáló helyiségek biztonsági zárhatóságáról gondoskodni kell.

23. Elektronikus adatfeldolgozási rendszer biztonsága

23.1. Biztonsági besorolás

134. Az Önkormányzat és a Hivatal az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény rendelkezéseinek megfelelően az E-ügyintézés rendszert biztonsági osztályba sorolja.

135. Az Önkormányzat és a Hivatal feladata minden E-ügyintézés rendszer biztonsági osztályához tartozó - az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendeletben meghatározott - követelményt érvényesíteni, annak érdekében, hogy a rendszer és a rendszerben kezelt adatok bizalmassági, sértetlenségi és rendelkezésre állási biztonsági kritériumai kockázatokkal arányos mértékben védve legyenek.

23.2. Fizikai biztonság

136. *[Gépterem]* Az E-ügyintézés rendszer kiszolgáló szerver infrastruktúrát a szerverszobában kell elhelyezni. A helyiségben biztosítani kell az informatikai eszközök megfelelő szintű fizikai védelmét (ujjlenyomatos beléptetés, riasztó, kamerák, klíma, szünetmentes áram stb.), illetve az eszközök optimális működésének környezeti feltételeit (klimatizálás, áramellátás stb.).

137. *[Irodahelyiségek]* Az irodahelyiségekben az ügyfélkapcsolati tevékenység ellátásához szükséges informatikai eszközök az alábbi módon:
   a) az ügyintéző a munkahelyén kizárólag az érintett adatait kezelje, a nem használt adatokat tegye el harmadik személy által hozzá nem férhető helyre,
   b) az informatikai eszközről ki kell jelentkezni vagy azt zárolni kell minden esetben, ha az ügyintéző a tevékenységét befejezte vagy megszakítja oly módon, hogy az informatikai eszköz felügyelet nélkül marad,
   c) az ügyfélszolgálaton minden esetben harmadik személy felügyeletét biztosítani kell annak érdekében, hogy ellenőrizetlenül ne férjen hozzá informatikai eszközhöz vagy egyéb adathordozóhoz,
   d) az ügyintéző ne változtassa meg az informatikai eszközök elhelyezését, akadályozza meg, hogy harmadik személy hozzáférjen az eszközhöz.

138. *[Karbantartás, hibajavítás]* A szerverszobába telepített fizikai védelmi rendszerek éves tervszerű megelőző karbantartásáról az Önkormányzatnak és a Hivatalnak kell gondoskodnia. A környezeti infrastruktúra valamely elemének meghibásodása észlelése és javítása az adott rendszer üzemeltetéséért felelős személy feladata.

23.3.Kiszolgáló rendszerek biztonsága

139. *[Technológiai védelem]* Az elektronikus ügyintézést támogató, kiszolgáló rendszerek esetében redundáns kiépítést kell biztosítani oly módon, hogy a kialakított architektúra összhangban álljon az Önkormányzat által megfogalmazott E-ügyintézés rendszerrel szemben támasztott rendelkezésre állási követelményekkel.

140. *[Hozzáférés védelem]* Az adatfeldolgozó tevékenységet támogató informatikai rendszerek hozzáférési alrendszerének az Önkormányzat hatályos Informatikai Biztonsági Szabályzat dokumentumában megfogalmazott hozzáférés védelmi követelményeket kell teljesíteniük.

141. *[Karbantartás]* Az Informatikai csoport felelőssége, hogy a szükséges karbantartási tevékenységek megtörténjenek. A karbantartási tevékenység hivatali munkaidőn kívüli időszakban, a szolgáltatás folyamatos fenntartása mellett történik.

142. Ha a karbantartás miatt az E-ügyintézés szolgáltatás szünetel – az Informatika csoport jelzése alapján - a Hivatal feladata elektronikus felületen tájékoztatni a felhasználókat a karbantartás várható időpontjáról, időtartamáról, továbbá amennyiben a karbantartás az E-ügyintézési rendszer részfunkcióját érinti csak, abban az esetben a tájékoztatónak tartalmaznia kell, hogy mely részszolgáltatások nem elérhetőek az elektronikus felületen.

143. Tekintettel arra, hogy a szoftverfrissítések, illetve javítókészletek telepítése jelentős mértékben befolyásolhatja az alkalmazások és informatikai eszközök működését, a frissítésekkel kapcsolatban az alábbi szabályokat kell betartani:

a) csak hiteles forrásból beszerzett frissítések alkalmazhatók,
b) a frissítés mellé csatolt dokumentációt a rendszergazdának át kell tanulmányoznia, hogy megismerje a telepítés várható következményeit,
c) abban az esetben, ha a frissítések telepítése a rendszer működőképességét vagy a tárolt adatok sértetlenségét veszélyezteti, akkor külön kiegészítő kockázatcsökkentő intézkedéseket kell alkalmazni a telepítést megelőzően.

144. A karbantartás végrehajtása után a rendszergazda felelőssége, hogy biztosított legyen a karbantartott informatikai eszköz fokozott felügyelete az esetlegesen felmerülő problémák miatt.

145. Az elvégzett karbantartásról a rendszergazdának feljegyzést kell készítenie és gondoskodnia kell a feljegyzés legalább 5 évig történő őrzéséről.

146. Az E-ügyintézés rendszer meghibásodása esetén a rendszergazda jogosult azonnali intézkedéseket foganatosítani.
A meghibásodott adathordozót a rendszergazda köteles megsemmisíteni. Ha a meghibásodás közvetlenül szolgáltatás kiesést okoz, akkor a Katasztrófa Elhárítási Terv alapján kell eljárni.

147. Olyan mentési megoldásokat kell alkalmazni, illetve olyan mentési eljárást kell működtetni, ami biztosítani tudja, hogy az informatikai eszközök sérülése, meghibásodása, illetve a tárolt adatok sérülése, használhatatlanná válása esetén rendelkezésre álljon olyan mentés, amely segítségével a kiesett informatikai szolgáltatás elfogadható időn belül újraindítható, illetve amelynek visszaállításával az elveszett adatmennyiség mértéke még kezelhető szinten marad.

148. Azon adatok esetén, amelyek hosszú távú megőrzését az Önkormányzat és a Hivatal elektronikus formában biztosítja a mentésnek alkalmasnak kell lennie az adatok jogszabályban előírt megőrzési idejének végéig történő visszaállítására. Ennek érdekében:

a) az adatok mentése, illetve archiválása mellett az adatok visszaállításához szükséges valamennyi egyéb adat (pl. konfigurációs paraméterek) és szoftver komponens is visszaállíthatóan mentésre, illetve archiválásra kerüljön vagy mentésük, illetve archivált állományuk létezzen,
b) az elkészített mentések tegyék lehetővé egy konzisztens állapot visszaállítását,
c) a mentett és az archív állományok adatainak a visszatöltéséhez szükséges berendezés mindenkor rendelkezésre álljon.

155. Mentésből történő adat visszatöltést a rendszergazda, illetve szakrendszer eseten annak rendszergazdája engedélyével lehet végrehajtani.

23.4. Elektronikus ügyintézés biztonsága

156. *[Általános biztonsági követelmények]* A biztosított elektronikus ügyintézési felület kialakítása során az alábbi biztonsági követelményeket kell betartani:

a) az elektronikus ügyintézési felület elérhetőségének biztonságos azonosíthatóságát elektronikus aláírás használatával kell biztosítani,
b) az ügyfél és az elektronikus ügyintézési felület között létrejött kommunikációs csatorna legyen erős titkosítással védve, biztosítva a személyes adatok titkosságát és sértetlenségét,
c) biztosítsa az elektronikus ügyintézési felületről az ügyfél által letöltött adatok sértetlenségét,
d) az ügyfelek tevékenysége kerüljön naplózásra, a naplózás tegye lehetővé az IP cím, idő és tevékenység szerinti keresését,
e) az elektronikus ügyintézési felület egyértelműen jelezzen vissza, hogy az ügyfél által indított tranzakció végrehajtása megtörtént-e.

157. *[Hozzáférés védelem]* Az elektronikus ügyintézési felületnek biztosítania kell egyedi authentikációs és authorizációs eljárást. Az elektronikus ügyintézési felület használatához előzetes regisztráció szükséges az ügyfelek által, mely regisztráció kapcsán az ügyfeleknek el kell fogadniuk a szolgáltatás használati feltételeit, illetve a vonatkozó adatvédelmi és adatkezelési szabályokat. A regisztráció nem jogosítja fel a felhasználókat az elektronikus ügyintézési szolgáltatások használatára, azok csak személyes azonosítást követően használhatók. Az elektronikus ügyintézési felület hozzáférés védelmi rendszerének biztosítani kell:

a) minden esetben a felhasználói azonosítók egyediségét,
b) hogy a felhasználó azonosítása felhasználónév és jelszó együttes megadásával történjen,
c) a felhasználók általi jelszóváltoztatás lehetőségét,
d) a jelszavak bonyolultságával kapcsolatos követelmények kikényszerítését,
e) a jelszavak meghatározott időközönkénti lejáratát,
f) sikertelen azonosítási kísérlet esetén a bejelentkezési lehetőség időtartamra történő tiltását,
g) a használt jelszavak erős titkosítással rejtjelezett formában történő továbbítását, ha a hozzáférési jogosultság elbírálása nem az informatikai eszközön történik és a hozzáférési adatok adathálózaton kerülnek továbbításra, kivéve az egyszer használatos jelszavak esetében,
h) a jelszavak rejtjelezett tárolását, azaz a hozzáférési rendszernek tilos bármilyen formában a jelszót megjeleníthetővé tennie, vagy egyszer használatos jelszó esetén azt generálni,
i) a felhasználói hozzáférések korlátozását meghatározott időszakra,
j) a hozzáférési rendszer tesztelt, biztonságilag ellenőrzött, általánosan használt módszert alkalmazzon,
k) csak az üzemeltető legyen képes módosítani a jogosultsági beállításokat.

158. *[Felhasználó kezelés]* Az elektronikus ügyintézési rendszer felhasználó kezelése részben automatikus, részben manuális módon kerül végrehajtásra. Az elektronikus ügyfélszolgálati rendszerhez érvényes felhasználói fiók regisztráció során automatikusan jön létre. Az elektronikus ügyfélszolgálati rendszer adminisztrációs felületéhez az Önkormányzat belső felhasználó kezelési eljárásrendjének megfelelően kerülnek létrehozásra az ügyintézői fiókok.

159. *[Naplózási és audit funkciók]* Az elektronikus ügyintézési rendszernek biztosítania kell, hogy a felhasználók által végrehajtott rendszeren belüli tevékenységek visszakereshetők legyenek, ennek érdekében a kialakított naplózási rendszernek biztosítania kell a felhasználó tevékenysége során végrehajtott módosított és eredeti rendszerállapot naplózását, rögzítve:

a) módosítást végrehajtó felhasználó nevét,
b) a módosítás dátumát és időpontját,
c) a módosított eredeti állapot értékét,
d) a módosítás utáni értéket.

160. Elektronikus ügyintézés során az adattörlés végrehajtójának azonosítóját, a végrehajtás idejét az adatfeldolgozó rendszerben visszakereshető módon naplózni kell, a naplóállományt 5 évig meg kell őrizni.

161. A kialakított naplózó rendszerrel szemben az alábbi biztonsági elvárásoknak kell teljesülniük:

a) a rendszer naplózza a sikeres és sikertelen felhasználói bejelentkezéseket,
b) a naplózandó események körét csak kiemelt felhasználói jogosultságokkal lehessen módosítani,
c) jelszó adatok ne kerüljenek semmilyen módon rögzítésre a naplóállományokban,
d) az alkalmazás rendelkezzen olyan adatfeldolgozó eszközökkel, melyek a naplóállományokban rögzített események feldolgozását elősegítik.

A rendszergazdának gondoskodnia kell a naplóállományok sértetlenségéről és megőrzéséről.

24. Rendszerfejlesztés és tesztelés biztonsága

162. A rendszerfejlesztési és tesztelési feladatok ellátására az Önkormányzatnak és a Hivatalnak az éles rendszertől külön álló informatikai rendszert kell fenntartania. Az Önkormányzat és a Hivatal elektronikus ügyintézési rendszer éles rendszerén fejlesztés, valamint tesztelés nem folytatható.

A fejlesztési tevékenység kapcsán az alábbiak szerint kell eljárni:

a) a fejlesztés tervezési szakaszában be kell vonni az információbiztonsági felelőst, akinek biztonsági szempontból jóvá kell hagynia a fejlesztést,
b) a fejlesztés során az elfogadott tervtől történő bármilyen eltérést dokumentálni kell, az eltéréseket jelezni kell az információbiztonsági referens felé, akinek jogában áll felülbírálni a változtatást,
c) törekedni kell, hogy a fejlesztő- és tesztrendszereken, tesztadatokon, vagy anonimizált éles adatokon történjen a tesztelés. Amennyiben éles adatok kerülnek átadásra a fejlesztő- és tesztrendszerekre és azok személyes adatokat is tartalmaznak, abban az esetben csak a rendszergazda engedélyével tölthetők át.
d) a fejlesztés tesztelésére szolgáló funkcionális tesztek végrehajtása az Önkormányzat és a Hivatal kijelölt szakterületeinek a feladata, a tesztelés eredményét jegyzőkönyvezni kell,
e) az információbiztonsági referens jogosult a fejlesztéssel kapcsolatban külön biztonsági tesztek végrehajtására,

f) a fejlesztés eredményét a rendszergazda veszi át, csak az átvétel után engedélyezett a fejlesztés alkalmazása az üzemi környezetben,
g) a fejlesztések minden egyes elkészült verzióját visszakereshető módon nyilván kell tartania,
h) a fejlesztés szerzői jogaival az Önkormányzat rendelkezik.

25. Védelmi rendszerek

163. *[Határvédelem]* Az Internet és a belső hálózat között határvédelmi eszköz működtetése kötelező. A határvédelmi eszköznek biztosítania kell, hogy

a) az Internet felől csak az Önkormányzat és a Hivatal által meghatározott adatkapcsolatok épülhessenek ki a kiszolgáló rendszerek felé,
b) az adatforgalom elsődleges vírus- és tartalomszűrése megvalósuljon,
c) a határvédelmi rendszer által kikényszerített biztonsági politikát a rendszergazdának rendszeres időközönként felül kell vizsgálnia. Olyan szabályok alkalmazása kötelező, amellyel biztosítható, hogy a szükséges minimum adatforgalom legyen engedélyezett külső hálózat irányából az Önkormányzat és a Hivatal belső informatikai rendszerei felé.

164. *[Vírusvédelem]* A rendszergazda feladata biztosítani többszintű vírusvédelmet, azaz a határvédelmi rendszeren kívül üzemeltessen vírusvédelmi rendszert. A vírusvédelmi rendszernek ki kell terjednie jelen szolgáltatásban érintett minden rendszerelemre. Az alkalmazott vírusvédelmi rendszernek biztosítania kell:

a) a központi menedzselhetőséget,
b) a vírus-adatbázis rendszeres és automatikus frissítését,
c) minden beérkező állományon történő vírusellenőrzést,
d) azon gyanúsnak ítélt, illetve kártékony kódra hasonlító jelsorozatok (nem írható vírusok) karanténba helyezését, melynek biztonságos eltávolítása nem lehetséges,
e) a vírusfertőzések, illetve fertőzött állományok kezelésének naplózását,
f) riasztások küldését az üzemeltetőnek.

VI. Fejezet
Záró rendelkezések

165. Jelen utasítás 2021. szeptember 15. napján hatályba.

166. Jelen utasítás hatályba lépésével egyidejűleg hatályát veszti a 2018. január 2. napja óta hatályban lévő Adatvédelmi és Adatbiztonsági Szabályzat.

Budapest, 2021. szeptember 13.

Soproni Tamás
polgármester

dr. Mogyorósi Sándor
jegyző