Budapest Főváros XIV. Kerület
Zuglói Polgármesteri Hivatal

1145 Budapest, Pétervárad u. 2.

Budapest Főváros XIV. Kerület Zugló Önkormányzatának Polgármestere és Jegyzője

5/2023. (V. 24.) együttes utasítása

Budapest Főváros XIV. Kerület Zugló Önkormányzata és a Zuglói Polgármesteri Hivatal adatvédelméről, adatbiztonságáról, adatkezelésének rendjéről

Horváth Csaba
polgármester

dr. Tiba Zsolt
jegyző

BUDAPEST FŐVÁROS XIV. KERÜLET ZUGLÓ POLGÁRMESTERE ÉS JEGYZŐJE

5/2023. (V. 24.) együttes utasítása Budapest Főváros XIV. Kerület Zugló Önkormányzata és a Zuglói Polgármesteri Hivatal adatvédelméről, adatbiztonságáról, adatkezelésének rendjéről

A jogalkotásról szóló 2010. évi CXXX. törvény 23. § (4) bekezdés c) pontjában meghatározott jogkörben eljárva, tekintettel az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény 25/M. § (1) bekezdés f) pontjában és 30. § (6) bekezdésében meghatározottakra és a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről szóló Európai Parlament és Tanács 2016/679 számú rendelet 24. cikk (2) bekezdésében vonatkozó szabályokra a következőket rendelem el.

I. Általános rendelkezések

1. Az utasítás célja, hatálya

1.§ Az Adatvédelmi és Adatbiztonsági Szabályzat (a továbbiakban: Szabályzat) célja, hogy meghatározza Budapest Főváros XIV. Kerület Zuglói Polgármesteri Hivatal (a továbbiakban: **Hivatal**) és Budapest Főváros XIV. Kerület Zugló Önkormányzata (a továbbiakban: **Önkormányzat**) által gyűjtött személyes adatok kezelése során irányadó adatvédelmi és adatbiztonsági eljárásrendet, felelősségi rendet. Célja továbbá a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről szóló Európai Parlament és Tanács 2016/679 számú rendelet (a továbbiakban: GDPR) és az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) rendelkezései alapján biztosítani, hogy a természetes személyek magánszféráját az adatkezelő tiszteletben tartsa, a közérdekű és a közérdekből nyilvános adatokat pedig mindenki megismerhesse és terjeszthesse.

2.§ (1) A Szabályzat személyi hatálya kiterjed a Hivatal köztisztviselői, ügykezelői, munkavállalói, közfoglalkoztatottai, az önkormányzati képviselők, a képviselő testület bizottságainak tagjai, a Hivatallal, Önkormányzattal megbízási jogviszonyban álló személyek (a továbbiakban: **foglalkoztatottak**) összességére.

(2) A Szabályzat tárgyi hatálya kiterjed a GDPR és az Infotv. által meghatározott, a Hivatal és az Önkormányzat által kezelt személyes adatokra, és adatkezelési tevékenységekre, azaz az utasítás rendelkezéseit kell alkalmazni bármely azonosított vagy azonosítható személyre vonatkozó információra. Annak eldöntése során, hogy egy személy azonosítható-e vagy sem, figyelembe kell venni minden lehetséges eszközt, amely valószínűsíthetően felhasználható az adott személy azonosítására.

(3) A Szabályzat előírásait alkalmazni kell a Hivatal belső szervezeti egységei által vezetett nyilvántartások, adatbázisok és valamennyi egyedileg kezelt személyes adat, továbbá dokumentum esetében.

3.§ (1) Az utasítás hatálya nem terjed ki - mint önálló adatkezelőkre – az Önkormányzat intézményeire és gazdasági társaságaira.

(2) A védelem szabályai nem alkalmazhatóak az olyan adatokra, amelyekkel – ún. anonimmá tételük következtében - az érintett többé nem azonosítható.

2. Értelmező rendelkezések

4.§ (1) A **GDPR** 4. cikk fogalom meghatározása alapján:

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

b) *adatkezelés*: a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés, továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összse

c) *álnevesítés*: a személyes adatok olyan módon történő kezelése, amelynek következtében további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik, feltéve hogy az ilyen további információt külön tárolják, és technikai és szervezési intézkedések megtételével biztosított, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet kapcsolni;

d) *nyilvántartási rendszer*: a személyes adatok bármely módon - centralizált, decentralizált vagy funkcionális vagy földrajzi szempontok szerint - tagolt állománya, amely meghatározott ismérvek alapján hozzáférhető;

e) *adatkezelő*: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza; ha az adatkezelés céljait és eszközeit az uniós vagy a tagállami jog határozza meg, az adatkezelőt vagy az adatkezelő kijelölésére vonatkozó különös szempontokat az uniós vagy a tagállami jog is meghatározhatja;

f) *adatfeldolgozó*: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel;

g) *címzett*: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, akivel vagy amellyel a személyes adatot közlik, függetlenül attól, hogy harmadik fél-e. Azon közhatalmi szervek, amelyek egy egyedi vizsgálat keretében az uniós vagy a tagállami joggal összhangban férhetnek hozzá személyes adatokhoz, nem minősülnek címzettnek; az említett adatok e közhatalmi szervek általi kezelése meg kell, hogy feleljen az adatkezelés céljainak megfelelően az alkalmazandó adatvédelmi szabályoknak;

h) *harmadik fél*: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely nem azonos az érintettel, az adatkezelővel, az adatfeldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére felhatalmazást kaptak;

i) *az érintett hozzájárulása*: az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez;

j) *adatvédelmi incidens*: a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi.

(2) Az Infotv. 3. § 5. és 6. pontja alapján

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

b) *közérdekből nyilvános adat:* a közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli;

c) *kötelezően közzéteendő közérdekű adat:* a Hivatal által kezelt és az lnfotv. 1. mellékletében, valamint egyéb jogszabályok alapján kötelezően nyilvánosságra hozandó információk körébe tartozó adat;

d) *közzététel:* az lnfotv.-ben meghatározott adatoknak internetes honlapon - www.zuglo.hu -digitális formában, bárki számára, személyazonosítás nélkül, korlátozástól mentesen, kinyomtatható és részleteiben is kimásolható módon, a betekintés, a letöltés, a nyomtatás, a kimásolás és a hálózati adatátvitel szempontjából is díjmentesen történő hozzáférhetővé tétele.

II. Az Önkormányzat testületeinek működésével, azok tagjainak tevékenységével összefüggő rendelkezések

5.§ (1) Az Önkormányzat Képviselő-testülete, valamint a Képviselő-testület bizottságai részére készülő előterjesztések, tájékoztatók és azok mellékletei személyes adatokat csak a jogszabály szerinti kötelezettség teljesítése érdekében és csak a jogszabály szerinti terjedelemben tartalmazhatnak.

(2) A Magyarország helyi önkormányzatairól szóló 2011. évi CLXXXIX. törvény (a továbbiakban: **Mötv**.) 46. § (2) bekezdése szerinti zárt ülés tartása esetén a zárt ülés keretében tárgyalható vagy tárgyalandó előterjesztéseket a zárt ülésen résztvevők vagy arra meghívottak ismerhetik meg.

(3) A személyes adatok védelmének biztosítása mellett zárt ülés tartása esetén is biztosítani kell a külön törvény szerinti közérdekű vagy közérdekből nyilvános adatok megismerését.

(4) Az önkormányzati képviselő jogosult mindazon adatok megismerésére, melyek képviselői munkájához szükségesek.

(5) A célhoz kötött adatkezelés elve alapján az önkormányzati képviselővel konkrét ügyben - az erre hatáskörrel rendelkező bizottság tagjaként, illetve a képviselő-testület ülésén - a személyes adatok kezelését igénylő eljárás részeként ismertethetők meg a személyes adatok.

(6) Amennyiben a képviselő, képviselői munkájával kapcsolatban személyes adatokhoz jut, vagy azzal összefüggésben adatot kezel, az adatvédelem biztosítása során az adatkezelővel azonos kötelezettségek terhelik.

6.§ (1) A zárt képviselő-testületi, bizottsági ülésen tárgyalandó önkormányzati hatósági ügyek tekintetében az előterjesztés a benyújtott egyéni kérelmek alapján készül, amely – figyelemmel az adatkezelés célhoz kötöttségének elvére – azokat az adatokat, információkat tartalmazza csak, amelyek elengedhetetlenül szükségesek a döntés meghozatalához. Az előterjesztést a döntés meghozataláig kizárólag a zárt ülésen résztvevők kaphatják meg. A zárt ülés napirendjeinek előterjesztésébe sem az ülés megtartása előtt, sem a döntés meghozatalát követően nem tekinthetnek be az állampolgárok.

(2) Azon természetes személyek, akik szociális helyzetükre tekintettel, szociális alapon bérelhetik az önkormányzat tulajdonában lévő lakást nem tekinthetőek az önkormányzattal üzleti kapcsolatban álló személyeknek, – így figyelemmel arra, hogy köztulajdont használnak – a nevükön és a bérleti jogviszony fennállására vonatkozó személyes adatukon kívül más adatuk nem minősül közérdekből nyilvánosnak.

(3) Azon magánszemélyek, illetve egyéb gazdasági tevékenységet folytató szervezetek, személyek esetében, akik piaci, üzleti alapon bérlői a köztulajdonban álló ingatlannak, ezért a nevük és a jogviszonyuk mellett a köztulajdont érintő és a bérleti jogviszonnyal összefüggő más adataik, így különösen a bérleti díj hátralékuk is közérdekből nyilvános adatnak minősülnek.

7.§ (1) A jegyző által vezetett szociális nyilvántartás adatait a Képviselő-testület tagjaival csak akkor és olyan körben ismertethetők meg, amennyiben a kérdéses ellátás odaítéléséről a képviselő-testület saját, illetve annak bizottsága átruházott hatáskörében dönt.

(2) A polgármester, a jegyző, a bizottság által átruházott hatáskörben meghozott szociális ellátást érintő döntéssel szembeni fellebbezésben szereplő személyes adatokat (a határozatokat és az eljárás iratait) a képviselő-testület tagja, jegyző, valamint az előkészítésben résztvevő hivatali munkatárs ismerheti meg.

(3) A polgármester, illetve a jegyző által az átruházott hatáskörében odaítélt támogatások címzettjéről, összegéről, illetve mértékéről, a képviselőnek csak zárt ülés keretében adható személyes adatokat is tartalmazó tájékoztatás, és csak abban a körben, amely a képviselői feladatainak ellátásával összefüggésben feltétlenül indokolt.

(4) A zárt ülés tartásának indokaira, vagyis a személyes adatok védelmére is figyelemmel a zárt ülés dokumentumainak, jegyzőkönyveinek megismerésére jogosultak arra illetékteleneknek nem adhatnak felvilágosítást az iratok tartalmáról és a bennük feltüntetett személyes adatokról, a megismert adatokat nem továbbíthatják, annak megtekintését nem tehetik lehetővé.

(5) A zárt ülésre készült, számukra átadott előterjesztést, a tájékoztatást, valamint a zárt ülésről készült jegyzőkönyvet a képviselőtestületi, illetve a bizottsági ülés résztvevői az érdemi döntést követően visszaszolgáltatják.

8.§ (1) A képviselő a polgármester, illetve a jegyző által kezelt, a szociális nyilvántartásba tartozó adatokat kizárólag akkor ismerheti meg, ha a polgármesteri határozattal szemben a fellebbezést terjesztenek elő, melynek elbírálására, a döntés meghozatalára a képviselő is jogosulttá,

illetve kötelezetté válik. Egyéb esetekben az adatok hozzáférhetővé tételére, továbbítására nincs törvényes mód.

(2) A zárt ülés anonimizált határozatait nyilvánosságra kell hozni, azokat bárki számára hozzáférhetővé kell tenni. A zárt ülés dokumentumaiban szereplő közérdekű és közérdekből nyilvános adat megismerhetőségét, az arra irányuló kifejezett kérés teljesítésével biztosítania kell.

III. Az adatkezelés, adatvédelem és adatbiztonság követelményrendszere

3. Felelősségi rend

9.§ Az adatkezelőt fokozott felelősség terheli az adatok jogszabályszerű kezeléséért, védelméért és szolgáltatásáért.

10.§ A foglalkoztatottak által végzett adatkezelésnek az adatkezelés minden szakaszában meg kell felelnie a GDPR-ban és az Infotv.-ben foglalt személyes adatok kezelésére vonatkozó elveknek.

11.§ (1) A Hivatal belső szervezeti egységei szakmai feladataik ellátása során kizárólag az adott feladat, a tevékenység megítélése, az adott döntés előkészítése érdekében, a vonatkozó jogszabályok rendelkezései alapján feltétlenül szükséges - és a személyes adatok körébe tartozó - adatok gyűjtését, tárolását, rendezését, felhasználását, nyilvánosságra hozatalát, archiválását, irattározását láthatják el.

(2) A Hivatal belső szervezeti egységei, az Önkormányzat és a Hivatal, tevékenységének átláthatóbbá tételét szolgáló, és a jogszabályok által közérdekűnek (nyilvánosnak) minősített adatok kezelését, majd ezek közzétételét köteles biztosítani.

12.§ (1) Az alapelvek érvényesülését biztosító eljárásrendek kidolgozásáért és betartatásáért az egyes belső szervezeti egységek vezetői (a továbbiakban együtt: **vezetők**) és a jegyző felelősek.

(2) Az adatkezelési eljárásrendeket a vezetők az adatvédelmi tisztviselő közreműködésével dolgozzák ki. Az eljárásrendeket, az adatvédelmi és az adminisztratív adatbiztonsági kockázatok feltérképezését és az adatkezelési elvek, szabályok alkalmazásának ellenőrzését a belső kontrollrendszer részeként kell kialakítani.

13.§ (1) A jegyző feladatkörében – a vezetők, foglalkoztatottak útján, illetve közreműködésével, továbbá előkészítő tevékenysége alapján – gondoskodik

a) a személyes adatok kezelésére vonatkozó alapelvek érvényesüléséről,

b) az adatkezelési műveletekre vonatkozó utasítások jogszerűségéről,

c) az adatok biztonságáról, az ehhez szükséges szervezési és technikai intézkedések meghozataláról, eljárási szabályok kialakításáról,

d) az adatvédelemmel összefüggő tevékenységek és felelősségek körültekintő és egyértelmű elhatárolásáról,

e) a Szabályzatban meghatározott feladatokhoz a szükséges erőforrások biztosításáról,

f) az adatvédelmi tisztségviselő kijelöléséről és munkájának ellenőrzéséről.

(2) Az Informatikai Osztály vezetője

a) felelős a Hivatalban végzett adatkezelés informatikai biztonságáért,

b) tárolja és őrzi valamennyi, a Hivatal informatikai biztonságára vonatkozó dokumentumot és adatbázist, beleértve az informatikai biztonsági politikát, valamint a biztonsági eseményekről készült adatbázist is,

c) kockázatelemzést végez az informatikai biztonságot érintő kérdésekben,

d) az informatikai biztonságot érintő gyakorlati kérdésekben tájékoztatja és irányítja az érintetteket annak érdekében, hogy elősegítse a megfelelő informatikai biztonsági szint elérését,

e) együttműködik az informatikai rendszerek üzemeltetőivel az informatikai működés folytonosságát biztosító terv elkészítésének érdekében.

(3) Az adatok biztonságát szolgáló intézkedéseket a technika mindenkori fejlettségére tekintettel kell meghozni, több lehetséges adatkezelési megoldás közül azt kell választani, amely a személyes adatok magasabb szintű védelmét biztosítja, kivéve, ha az aránytalan nehézséget jelentene.

4. Az adatvédelem tárgya

14.§ Az adatvédelem folyamatában a védelem tárgya:

a) a Hivatal működése során keletkezett személyes adatok teljes köre, keletkezésüktől a megsemmisítésükig,

b) az adathordozók, fizikai jellegüktől függetlenül, amelyek személyes adatokat tartalmaznak; az adathordozók lehetnek papír alapú iratok, kimutatások, listák, térképek, műszaki dokumentációk, elektronikus, optikai és mágneses adathordozók, adattároló és adatkezelő informatikai rendszerek a vonatkozó informatikai szabályozás részletezése szerint;

c) az a fizikai környezet, ahol az adatállomány kezelése, tárolása történik.

5. A személyes adatok kezelésére vonatkozó elvek érvényesítése

15.§ A GDPR 5. cikkével összhangban az adatkezelés során a Hivatal az alábbi elvek érvényesülését tartja szem előtt

a) jogszerűség, tisztességes eljárás, átláthatóság,
b) célhoz kötöttség,
c) adattakarékosság,
d) pontosság,
e) korlátozott tárolhatóság
f) integritás és bizalmas jelleg,
g) elszámoltathatóság.

6. A célhoz kötöttség, adattakarékosság, pontosság, korlátozott tárolhatóság elvek érvényesülésének biztosítása

16.§ A vezetők kötelesek gondoskodni arról, hogy a jogszabályon alapuló adatkezelés célhoz kötötten, a szükségesség és arányosság elve alapján indokolható minimális körben, pontos, ak-

tuális adattartalommal és a szükséges vagy jogszabály által meghatározott időtartamra történjen. A vezetők az adatvédelmi tisztviselővel együttműködve kötelesek ellenőrizni ennek betartását a kialakított munkafolyamatok esetében jogszabályváltozás esetén vagy szükség szerint, továbbá az új munkafolyamatok kialakítása során az új munkafolyamat bevezetése előtt minden esetben.

7. Integritás, bizalmas jelleg elv érvényesülésének biztosítása

17.§ (1) Az adatkezelés vagy adatbiztonság valamely elve sérülésének gyanúja esetén a foglalkoztatott köteles értesíteni közvetlen vezetőjét az incidens kivizsgálása és kezelése érdekében. A vezető köteles értesíteni a jegyzőt és az adatvédelmi tisztviselőt minden olyan esetben, amikor incidens történt, különösen abban az esetben, ha az incidens nagy mennyiségű személyes adatot érint vagy különleges személyes adatot érint.

(2) Informatikai adatbiztonság sérülésének gyanúja esetén minden esetben értesíteni szükséges az incidensről az informatikai biztonsági vezetőt is.

(3) Az adatvédelmi incidens feltárása és kezelése, jövőbeli megelőzése érdekében lefolytatásra kerülő eljárásban a foglalkoztatottak kötelesek közreműködni.

8. Elszámoltathatóság elve érvényesülésének biztosítása

18.§ (1) A megfelelő szintű adatkezelési tudatosság kialakítása és fenntartása érdekében oktatásokat kell tartani

a) jogszabályváltozás esetén a jogalkalmazást megelőzően,

b) szervezeti egység vezetője hatáskörében kezelhető adatkezelési szabálytalanság esetén az esemény kezelését követően haladéktalanul, vagy

c) hivatali szinten kezelendő adatkezelési szabálytalanság esetén a szabálytalanság kezelését követően haladéktalanul.

(2) Az (1) bekezdésben foglaltakon túl a foglalkoztatottak részére évente legalább egyszer az adatvédelmi tisztviselő adatvédelemről és adatbiztonságról oktatást tart.

(3) Az Informatikai Osztály vezetője évente legalább egy alkalommal oktatást tart az informatikai biztonságról.

(4) Az oktatásokat és a belső kontrollrendszer részeként elvégzett adatvédelmi feladatokat dokumentálni szükséges.

9. A személyes adatok kezelésére vonatkozó elvek érvényesítése

19.§ (1) A 15.§-ban nevezett alapelvek érvényesülése és érvényesítése érdekében az önkormányzati feladatok ellátása során az adott feladat szerinti ügymenet részeként biztosítani kell az adatkezelés szabályainak maradéktalan betartását, a természetes személyek adatainak a védelmét a jogellenes felhasználástól.

(2) Az adatkezelés során biztosítani kell:

a) az egyén szempontjából fontos adatok helyes, pontos kezelését, a hibás adat előfordulása esetén annak észlelésekor hivatalból, valamint az érintett kezdeményezésekor a pontosítást haladéktalanul teljesíteni kell;

b) hogy az adott személy adatai kizárólag a jogszabály rendelkezéseivel összhangban kerüljenek feldolgozásra, rögzítésre, felhasználásra, valamint ne kerüljenek illetéktelenek birtokába;

c) hogy a személyes adatoknak a közérdekű adatokkal való együttes alkalmazásuk esetén ne akadályozzák a közérdekű adatok nyilvánosságát, szolgáltatását, de a személyes adat védelme biztosított legyen;

d) a személyes adatok tekintetében minden esetben a zárt kezelést és a jogszabályok szerinti előírásoknak megfelelő hozzáférést;

e) a különböző célú adatok, adatállományok és adatbázisok folyamatos vezetését, aktualizálását és az adathordozó fajtájától független folyamatos rendelkezésre állását és elérhetőségét az arra jogosultak számára;

f) a különböző adatok, adatállományok és adatbázisok valódiságát, pontosságát, részletességét, hitelességét;

g) hogy a hiányos, a pontatlan, a régi adatok pontosításra, aktualizálásra, és az idejét múlt adatok törlésre kerüljenek;

h) a Hivatal informatikai és információs rendszereinek, adatbázisainak folyamatos működését, és szükség szerinti folyamatos hozzáférés lehetőségét, a folyamatos aktualizálást, a közérdekű adatok folyamatos, a jogszabályoknak megfelelő szolgáltatását, az érdeklődök véletlenszerű internet kapcsolódására az elektronikus adatok folyamatos rendelkezésre állásának a garantálását; valamint

i) az adatok, adatállományok és adatbázisok – akár számítógépes, akár manuális – fizikai biztonságát.

10. Az adatkezelés jogalapja

20. § (1) A személyes adatok kezelése kizárólag akkor és annyiban jogszerű, amennyiben az alábbi feltételek legalább egyike teljesül:

a) az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez;

b) az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél, vagy az a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges;

c) az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges;

d) az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges;

e) az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges;

f) az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei

vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé, különösen, ha az érintett gyermek.

(2) Az (1) bekezdés f) pontja nem alkalmazható a közhatalmi szervek által feladataik ellátása során végzett adatkezelésre.

21.§ (1) A személyes adatok kezelése során figyelemmel kell lenni arra a Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: **NAIH**) által rögzített általános érvényű álláspontra is, hogy a közhatalmi tevékenységet vagy egyéb közfeladatot ellátó szerv – mint költségvetési szerv – minden közjogi és magánjogi jogviszonyának, és az ahhoz járulékosan kapcsolódó adatkezelési jogviszonyainak kizárólag közfeladatai ellátásával összefüggésben lehet alanya, ettől eltérő minősége fogalmilag kizárt. Ebből fakadóan e jogalap, mintegy magába olvasztja, elnyeli a további adatkezelési jogalapokat.

(2) Az általános szabály szerint a Hivatal valamennyi adatkezelésének a jogalapja a GDPR 6. cikk (1) bekezdés e) pontja, azaz az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges.

(3) A 20. § (1) bekezdésben meghatározott jogalapok közül más jogalapot csak abban az esetben lehet az adatkezelés jogalapjául választani, ha a GDPR 6. cikk (1) bekezdés e) pontja kivételesen nem alkalmazható.

22.§ Az egyes ügytípusokhoz kapcsolódó adatkezelési tájékoztatók készítése során a GDPR 39. cikk (1) bekezdés a) pontja szerint minden esetben ki kell kérni a Hivatal adatvédelmi tisztviselőjének szakmai állásfoglalását, tanácsát.

IV. Adatvédelem és adatbiztonság a munkahelyi feladatellátás során

11. Adminisztratív és informatikai adatbiztonság

23.§ Az adatkezelő köteles gondoskodni az általa kezelt adatok adminisztratív és informatikai biztonságáról. Az adatokat védeni kell a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés vagy sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen.

24.§ A foglalkoztatott köteles a megőrzésre, illetve irattározásra nem kerülő és feleslegessé vált iratok és egyéb nyomtatványok, feljegyzések megsemmisítésére, melyet – ahol rendelkezésre áll – irodai megsemmisítővel kell végrehajtani. A papírvagdalék a kommunális szemétbe üríthető.

25.§ (1) Nagy mennyiségű felesleges papírt, ahol nem áll rendelkezésre irodai megsemmisítő, át kell adni a Gondnoksági Osztály részére megsemmisítésre.

(2) A Hivatal épületének folyosóin a megsemmisítendő irat gyűjtésére szolgáló tároló dobozok vannak kihelyezve. Ezek rendszeres ürítéséről a Gondnoksági Osztály gondoskodik.

(3) Szükség esetén egyedi kérésre a Gondnoksági Osztály munkatársai begyűjtik a megsemmisítésre elkülönített nagyobb mennyiségű papírt, azonban a begyűjtésig azt zárt helyen kell tárolni.

(4) A kommunális szemétbe, papírkosárba ép vagy rekonstruálható formában nem kerülhet személyes, vagy egyéb okból nem nyilvános adatot hordozó papír.

(5) Az irattári selejt ellenőrzött megsemmisítésére a Hivatal külső vállalkozóval is megállapodhat.

26.§ (1) Személyes, vagy egyéb okból nem nyilvános adatot hordozó papír nem maradhat folyosón vagy egyéb, kulccsal nem zárható helyen őrizetlenül. Az irodákat – a kulcskezelésre vonatkozó külön utasításban közzétett szabályzat előírásaira tekintettel – e szempontból zárható helynek kell tekinteni.

(2) Az ügyiratok munkaidőben sem hagyhatók asztalon vagy nyílt tárolásban az utcai vagy udvari ablakok közelében, ha arra közelről rálátás lehetséges.

27.§ (1) A Hivatal irodáit munkaidőn kívül, illetve munkaidőben, a munkatársak távollétében kulcsra zárva kell tartani, a kulcsot a kulcskezelésre vonatkozó külön utasításban közzétett szabályzatra is tekintettel biztonságosan kell tárolni.

(2) A vas iratszekrényeket, lemezszekrényeket az iroda elhagyása esetén munkaidőben is zárni kell, a kulcsot a kulcskezelésre vonatkozó külön utasításban közzétett szabályzatra is tekintettel biztonságosan kell tárolni.

28.§ (1) Személyes adatok továbbítása során az adatkezeléssel megbízott ügyintéző és az iratkezelésért, postázásért felelős szervezeti egység együttesen felelősek azért, hogy az adatok felfedés nélkül – így ép, lezárt borítékban, csomagban, hogy a küldemény érdemi szövege ne legyen kívülről olvasható – továbbításra kerüljenek a címzett részére.

(2) Az (1) bekezdésben rögzített felelősség a küldeménynek a posta részére történő átadásig tart.

29.§ A Hivatal területén őrizetlenül hagyott, illetve elveszett, majd megtalált, a Hivatal valamely szervezeti egységéhez tartozó iratok esetén elsődlegesen az érintett szervezeti egység beazonosítását kell megkísérelni. Amennyiben a beazonosítás sikeres, a megtalált iratot át kell adni az érintett szervezeti egység vezetőjének. Amennyiben a beazonosítás nem lehetséges, úgy az Ügyfélszolgálati Osztály őrzi a személyazonosságát igazoló érintett, vagy képviselője, gondnoka, megbízottja részére történő átadásig.

30.§ (1) Személyes adatokat tartalmazó hivatalos iratok nyomtatása elsődlegesen az irodákban lehetséges. Ahol nincs irodában elhelyezett nyomtató vagy nagyobb mennyiségű irat nyomtatása szükséges, úgy a Hivatal folyosóin elhelyezett nyomtatók használandók.

(2) A folyosón elhelyezett nyomtatóval személyes adatot tartalmazó iratot nyomtatni a foglalkoztatott egyedi azonosítását követően – egyedi jelszó beírásával- és kizárólag a foglalkoztatott jelenlétében lehetséges. A foglalkoztatottnak meg kell várnia, amíg a nyomtatás befejeződik. Kinyomtatott anyagot a nyomtatóban őrizetlenül hagyni tilos.

31.§ Az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény alapján a kötelező elektronikus ügyintézés hatálya alá tartozó szervek között a személyes adatok továbbítása hivatali kapun keresztül történik.

32.§ A Hivatal az adatnyilvántartások rendszerének felépítése, a jogosultságok meghatározása, és egyéb szervezeti intézkedések útján gondoskodik arról, hogy a személyes adatokat tartalmazó iratokat csak azok a foglalkoztatottak, illetve egyéb, a Hivatal vagy az Önkormányzat képviseletében eljáró személyek ismerhessék meg, akiknek erre munkakörük, feladatuk ellátása érdekében szükségük van.

33.§ Személyes adatot tartalmazó Word fájlt, Excel táblázatot vagy más fájlt elektronikus levélben egyéb címzett részére kizárólag jelszó védelemmel lehet küldeni vagy a részére más elektronikus módon elérhetővé tenni. A címzett részére a küldött Excel táblázat megtekintéséhez szükséges jelszó külön elektronikus levélben vagy telefonon keresztül adható meg.

34.§ (1) A Hivatal épületéből főszabályként tilos ügyiratot kivinni.

(2) Az ügyintéző által otthoni munkavégzéshez szükséges személyes adatot tartalmazó iratot csak megfelelően erős jelszóval védett adathordozóra lehet kimenteni. Az adathordozó megfelelő szintű védelméért, az azon tárolt adatok biztonságáért az érintett foglalkoztatott felel.

35.§ Az adatállományok, számítógépek, adathordozók, programok informatikai védelmére, az adatok biztonságos informatikai kezelésére, őrzésére, mentésre, törlésre, archiválásra, helyreállításra, a hozzáférési jogosultságok beállítására, a biztonságos jelszavak kialakítására, a vírusvédelemre az Informatikai Biztonság Szabályzat rendelkezései az irányadóak.

36.§ (1) Amennyiben a hivatali munkavégzés azt indokolttá teszi – így különösen a képviselő-testületi ülésen, a bizottsági üléseken, a nemzetiségi önkormányzat ülésein és egyéb külső helyszínen történő munkavégzés esetén – a személyes adatok biztonsága érdekében kiemelt körültekintéssel kell eljárni. Ennek során az iratokat az adattakarékosság elvére figyelemmel kell előkészíteni úgy, hogy az irat csak a döntés meghozatalához szükséges személyes adatokat tartalmazza, továbbá az egyéb személyes adatokat anonimizálni kell. A Hivatal épületéből kivitelre szánt iratokat zárható mappába elhelyezve, lehetőség szerint két foglalkoztatott közreműködésével – kik közül az egyik lehetőleg a Hivatal honvédelmi és közbiztonsági referense – kell szállítani.

(2) A külső helyszínen történő munkavégzés befejezetését követően az iratok Hivatalba történő biztonságos visszaszállításáról gondoskodni kell az (1) bekezdésben meghatározottak szerint.

12. Adatvédelem az ügyfelekkel történő kapcsolattartás során

37.§ A személyes adatok kezelésével kapcsolatos ügyekben csak a Hivatal szervezeti és működési szabályzatában meghatározott feladatkör szerint illetékes belső szervezeti egység járhat el, működhet közre.

38.§ Az ügyintéző csak az egyazon ügyben érdekelt ügyfeleket fogadhatja együttesen, ellenkező esetben egyesével kell foglalkozni az ügyfelekkel. Ügyintézés alatt - az iratbetekintés szabályainak figyelembe vételével - az érintett törvényes képviselője, gondnoka, meghatalmazottja, jogi képviselője, - továbbá adatkezelési tájékoztatáson alapuló kifejezett beleegyezésével - a kíséretében levő személy is jelen lehet.

39.§ A személyes adatokat tartalmazó ügyek esetében az illetékes szervezeti egység vezetője, illetve a szignálás során az általa kijelölt ügyintéző illetve valamennyi közreműködő felelős azért, hogy az adott iratanyag illetéktelenek kezébe ne kerülhessen, és az ügy intézése, a jogorvoslati eljárás, a testületek elé terjesztés valamennyi mozzanata jogszerű legyen és dokumentálásra kerüljön. A folyamatos ügyintézés érdekében a megfelelő helyettesítésről gondoskodni kell, és ezt az érintett ügyintéző munkaköri leírásában rögzíteni kell.

40.§ Ügyfél és a kíséretében levő személyek csak az ügyintéző jelenlétében tartózkodhatnak az irodában, várakozásra az ügyfélteret - váró, folyosó - vehetik igénybe.

41.§ Telefonon történő hivatalos beszélgetést zárt ajtók mögött, ügyfelek kizárásával kell folytatni. Az ügyfél jelenlétében csak a saját ügyében folytatható hivatalos telefonbeszélgetés. Ezen túlmenően csak általános jellegű információ továbbítható harmadik személy részére.

42.§ Több ügyintéző közös irodai elhelyezése esetén, több ügyben az egyidejű ügyfél fogadást kerülni kell. Ha a több ügyfél különböző időpontokban történő fogadása nem valósítható meg, akkor az ügyek úgy intézhetőek, hogy az egyes ügyek ügyfelei a másik ügyéről, annak ügyfeléről, adatairól tudomást ne szerezhessenek, továbbá az érintett beleegyezésével folytatható ügyében telefonbeszélgetés.

43.§ Nem azonosított ügyfél, telefonáló, elektronikus levelet küldő nem kaphat az ügyekről érdemi információkat, sem személyes adatokat. Azonosítatlan személy - aki a telefonon keresztül történő kapcsolatfelvétel, illetve az email címe alapján nem azonosítható minden kétséget kizáróan - csak általános tájékoztatásban részesülhet, illetve számára közérdekű adatok adhatók ki.

44.§ Ügyfél részére személyes adatot tartalmazó érdemi döntés és egyéb személyes adatot tartalmazó irat kizárólag ügyfélkapun keresztül vagy postai úton küldhető, továbbá személyesen, vagy igazolt képviselő vagy meghatalmazottja útján vehető át, ezen iratokat elektronikus levélben küldeni – a 45. §-ban írtak kivételével – nem lehet.

45.§ Amennyiben egy adott ügyben sem a személyes átvétel, sem az ügyfélkapun történő küldés nem lehetséges, és a személyes adatot is tartalmazó irat elektronikus levélben kerül megküldésre a címzett részére, úgy jelen szabályzat 33. §-ában foglaltak szerint kell eljárni.

46.§ Ha jogszabály eltérően nem rendelkezik, adatszolgáltatás személyes adatokat tartalmazó adatbázisból oly módon történhet, hogy

a) az érintett a Hivatal vagy az Önkormányzat által kezelt saját személyes adataiba betekinthet, arról tájékoztatást kérhet úgy, hogy ezalatt más természetes személy személyes adatait nem ismerheti meg;

b) az érintett megkeresésére válaszolva, személyes adatokat szolgáltató okiratot személyenként kell elkészíteni és iktatni, amennyiben ez nem lehetséges, az iratot anonimizálni szükséges.

13. Szerződések adatvédelmi rendelkezései, adatfeldolgozói szerződések

47.§ Személyes adatok kezelését eredményező szerződések adatvédelmi rendelkezései szövegezéséhez a szerződés előkészítése során az adatvédelmi tisztviselő tanácsát ki kell kérni.

14. Számítástechnikai és egyéb adatkezelésre alkalmas eszközök munkahelyi használata

48.§ (1) A foglalkoztatott a rendelkezésére bocsátott munkaeszközt kizárólag munkavégzés céljából használhatja.

(2) Ha a foglalkoztatott a számítástechnikai eszközön az (1) bekezdésében meghatározottakkal ellentétben munkaviszonnyal össze nem függő személyes adatot tárol, a munkáltató a magánszférát tiszteletben tartva köteles eljárni, így nem kezelheti az ily módon tárolt személyes adatot, továbbá lehetőséget kell biztosítania a foglalkoztatott számára a magánadatokkal való rendelkezésre.

(3) A munkáltató a foglalkoztatottaknak a munkavégzés céljából rendelkezésre bocsátott munkaeszközök - számítógép, mobil készülék, laptop, nyomtató, tablet- használatát jogosult ellenőrizni. Az ellenőrzés a munkavégzéssel összefüggő indokolt célból történhet.

(4) Az ellenőrzésnek az elérni kívánt céllal arányosnak kell lennie, nem sértheti a foglalkoztatott alapvető jogait.

(5) A foglalkoztatott által használt munkaeszköz munkáltató általi ellenőrzése akkor jogszerű, ha az ellenőrzés pontos részleteiről, az ellenőrzést megelőzően a GDPR előírása szerinti formában és módon tájékoztatják a foglalkoztatottat. Az ellenőrzésről jegyzőkönyvet kell felvenni.

49. § (1) Az adatbiztonság vagy az informatikai rendszer védelme okán az informatikai hálózatot üzemeltető, fenntartó rendszergazda vagy informatikus az informatikai vagy egyéb eszköz tartalmába jogosult betekinteni. Az így megismert adatokat harmadik személy számára – így a munkáltató részére – nem jogosult továbbítani.

(2) Az (1) bekezdésben foglaltaktól eltérően, ha olyan adatra, információra bukkan, amely valamely jogszabály, így különösen a büntető törvénykönyvről szóló 2012. évi C. törvény rendelkezéseibe ütközik. Ebben az esetben, nem bűncselekményre utaló körülmény észlelése esetén a szervezeti egység vezetőjét, továbbá a jegyzőt haladéktalanul értesíteni kell a további intézkedések megtétele céljából, és az észlelésről hivatalos feljegyzést kell felvenni. Bűncselekményre utaló körülmény észlelése esetén a jegyzőt haladéktalanul értesíteni kell a további intézkedések megtétele céljából, és az észlelésről hivatalos feljegyzést kell felvenni.

V. Érintetti jogok érvényesülése

50. § (1) A GDPR 6. cikk (1) bekezdés e) pontja szerinti jogalap esetén az érintettet a GDPR 13. és 14. cikke szerint megilleti a *hozzáféréshez való jog*.

(2) Az érintett jogosult arra, hogy a Hivataltól tájékoztatást kérjen arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e, és ha ilyen adatkezelés folyamatban van, jogosult arra, hogy megismerje azt, hogy a Hivatal mely személyes adatait, milyen jogalapon, milyen adatkezelési cél miatt, mennyi ideig kezeli. A Hivatal kinek, mikor, milyen jogszabály alapján, mely személyes adataihoz biztosított hozzáférést vagy kinek továbbította a személyes adatait, milyen forrásból származnak a személyes adatai, történik-e automatizált döntéshozatal.

(3) A Hivatal az adatkezelés tárgyát képező személyes adatok másolatát az érintett erre irányuló kérésére első alkalommal díjmentesen bocsátja a rendelkezésére, ezt követően adminisztratív költségeken alapuló, ésszerű mértékű díjat számíthat fel. Az adatbiztonsági követelmények teljesülése és az érintett jogainak védelme érdekében a Hivatal köteles meggyőződni az érintett és a hozzáférési jogával élni kívánó személy személyazonosságának egyezéséről, ennek érdekében a tájékoztatás, az adatokba történő betekintés, illetve azokról másolat kiadása is az érintett személyének azonosításához kötött.

51. § (1) A GDPR 6. cikk (1) bekezdés e) pontja szerinti jogalap esetén az érintettet a GDPR 16. cikke szerint megilleti a *helyesbítéshez való jog*.

(2) Az érintett kérheti, hogy a Hivatal módosítsa valamely személyes adatát. Amennyiben az érintett hitelt érdemlően igazolni tudja a helyesbített adat pontosságát, a Hivatal a kérést legfeljebb egy hónapon belül teljesíti, és erről az általa megadott elérhetőségen értesíti az érintett személyt.

52.§ (1) A GDPR 6. cikk (1) bekezdés e) pontja szerinti jogalap esetén az érintettet a GDPR 18. cikke szerint megilleti a *zároláshoz (adatkezelés korlátozásához) való jog*.

(2) Az érintett személy kérheti, hogy az adatkezelés korlátozott jellegének egyértelmű jelölésével és az egyéb adatoktól elkülönített kezelés biztosításával a személyes adatai kezelését a Hivatal korlátozza amennyiben:

a) vitatja a személyes adatai pontosságát;

b) - az adatkezelés jogellenes, és az érintett ellenzi az adatok törlését, és ehelyett kéri azok felhasználásának korlátozását;

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

d) az érintett tiltakozott az adatkezelés ellen.

(3) A (2) bekezdés a) pontja szerinti esetben a Hivatal arra az időtartamra korlátozza az adatkezelést, amíg ellenőrzi a személyes adatok pontosságát. A (2) bekezdés d) pontja szerinti esetben a korlátozás arra az időtartamra vonatkozik, amíg megállapításra nem kerül, hogy az adatkezelő jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben.

53.§ (1) A GDPR 6. cikk (1) bekezdés e) pontja szerinti jogalap esetén az érintettet a GDPR 21. cikke szerint megilleti a *tiltakozáshoz való jog*.

(2) Az érintett személy bármikor tiltakozhat az adatkezelés ellen, ha álláspontja szerint a Hivatal a személyes adatát nem az adatkezelési tájékoztatóban megjelölt céllal összefüggésben kezeli. Ebben az esetben a Hivatalnak kell igazolnia, hogy a személyes adat kezelését olyan kényszerítő erejű jogos okok indokolják, amelyek elsőbbséget élveznek az érintett érdekeivel, jogaival és szabadságaival szemben, vagy amelyek jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódnak.

54.§ (1) A GDPR 6. cikk (1) bekezdés e) pontja szerinti jogalap esetén az érintettet a GDPR 17. cikke szerint megilleti a *törléshez való jog*.

(2) Az érintett csak akkor élhet a törléshez való jogával, ha a Hivatalra ruházott közhatalmi jogosítványok gyakorlása keretében végzett, vagy a Hivatal közérdekű feladatainak végrehajtásához az adat nem szükséges.

55.§ (1) A GDPR 6. cikk (1) bekezdés e) pontja szerinti jogalap esetén az érintettet a GDPR 77. és 79. cikke szerint megilleti a *jogorvoslathoz való jog*.

(2) Az érintettet tájékoztatni kell, hogy ha úgy ítéli meg, hogy a Hivatal a személyes adatainak kezelése során megsértette a hatályos adatvédelmi követelményeket, akkor:

a) panaszt nyújthat be a Nemzeti Adatvédelmi és Információszabadság Hatósághoz, elérhetősége jelenleg cím: 1055 Budapest, Falk Miksa utca 9-11., postacím: 1374 Budapest, Pf. 603., E-mail: ugyfelszolgalat@naih.hu; honlap: www.naih.hu. Az elérhetőség változása esetén az aktuális adatokat kell használni.

b) lehetősége van adatainak védelme érdekében bírósághoz fordulni, amely az ügyben soron kívül jár el. Ebben az esetben szabadon eldöntheti, hogy a lakóhelye (állandó lakcím) vagy a tartózkodási helye (ideiglenes lakcím), illetve a Hivatal székhelye szerint illetékes törvényszék-

nél nyújtja-e be keresetét. A lakóhelye vagy tartózkodási helye szerinti törvényszéket megkeresheti a http://birosag.hu/ugyfelkapcsolatiportal/birosag-kereso.hu oldalon. A Hivatal székhelye szerint a perre a Fővárosi Törvényszék rendelkezik illetékességgel.

VI. Térfigyelő kamerák alkalmazása

56.§ (1) Hivatal adat - és vagyonbiztonsága érdekében a Hivatal épületeiben, zárt udvarán és a be-járatokat figyelő zártláncú térfigyelő kamerarendszert üzemeltet. A hivatali kamerákkal kapcsolatos adatkezelésre külön adatkezelési tájékoztató vonatkozik, amely az alábbi linken érhető el: http://info.zuglo.hu/adatkezelesi_tajekoztato.pdf?r

(2) A Hivatalba belépő új foglalkoztatottakkal a térfigyelő kamerákra vonatkozó adatkezelési tájékoztató megismertetése a Humánpolitikai Osztály feladata és kötelessége.

VII. Elektronikus beléptető rendszer

57.§ (1) Az Önkormányzat vagyonának védelme céljából a Hivatal elektronikus beléptető rendszert működtet.

(2) A beléptető rendszer a belépő és kilépő személy nevét, munkakörét, az épületbe történő belépés és kilépés kezdő időpontját, az épületben eltöltött időtartamot, valamint a belépés és kilépés helyszínét rögzíti.

(3) Az elektronikus beléptető rendszerben tárolt személyes adatokhoz – beleértve az alkalmazottak belépési adatait is – az Üzemeltetési Főosztály vezetője, az Informatikai Osztály vezetője és az általa kijelölt munkatársa fér hozzá belépési kártya készítése céljából, valamint az élőerős őrzést ellátó foglalkoztatottak, akik a belépés és kilépés idején láthatják az adatokat.

(4) Az adatok kizárólag célhoz kötötten használhatóak fel, azok nem használhatóak fel profilalkotásra, és nem továbbíthatók.

(5) Statisztikai célokra kizárólag visszafejtésre alkalmatlan anonimizált vagy álnevesített formában használhatóak fel az adatok.

(6) A beléptető rendszerben tárolt adatok 6 hónap elteltével automatikusan törlődnek, továbbá a foglalkoztatotti jogviszony megszűnését követően a beléptető rendszerben tárolt személyes adatokat haladéktalanul törölni kell.

VIII. Az adatkezelési tevékenység nyilvántartása

58.§ Az adatvédelmi tisztviselő a Hivatal adatkezelési tevékenységéről a GDPR 30. cikke szerinti tartalommal adatkezelési nyilvántartást vezet. A nyilvántartás az *„F meghajtó adatleltár_nyilvántartás adatkezelési műveletekről”* nevű mappájában érhető el, melyhez az adatvédelmi tisztviselő rendelkezik hozzáférési jogosultsággal.

59.§ Az adatvédelmi tisztviselő legalább 3 évente, de a vonatkozó jogszabályváltozást követően haladéktalanul felülvizsgálja, aktualizálja az adatleltárt.

60.§ A vezető köteles együttműködni az adatvédelmi tisztviselővel az adatkezelési tevékenységek nyilvántartásának felvételében és felülvizsgálatában, köteles továbbá határidőben pontos adatokat átadni az adatvédelmi tisztviselő részére.

61.§ (1) A vezető az új adatkezelési tevékenységet, annak megkezdését megelőzően, vagy a már folyamatban lévő adatkezelés körülményeiben bekövetkező változást a nyilvántartás szerinti adatkörök vonatkozásában, haladéktalanul köteles bejelenteni az adatvédelmi tisztviselőnek az adatvedelem@zuglo.hu címen.

(2) A bejelentés alapján az adatvédelmi tisztviselő az új adatkezelési tevékenységet rögzíti, vagy módosítja a nyilvántartásban szereplő adatokat. Szükség esetén az illetékes szervezeti egységgel is konzultál.

62.§ (1) Az adatkezelési nyilvántartás felvételéhez a vezető adatkezelési kérdőívet tölt ki.

(2) Az adatvédelmi tisztviselő az adatkezelési kérdőív alapján áttekinti a szervezeti egységek belső kontrollrendszerben rögzített folyamatait a vezetőkkel, és összeállítja az adatkezelési tevékenységek nyilvántartását.

(3) Az adatkezelési nyilvántartás alapján az adatvédelmi tisztviselő elkészíti az érintettek számára az adatkezelési tájékoztatókat. A nyilvántartásban történő módosítás esetén az adatkezelési tájékoztató érintett pontjait is felül kell vizsgálni, szükség esetén azokat is módosítani kell.

(4) Az adatkezelési tájékoztatót a szervezeti egységek elhelyezését szolgáló hivatali részen, valamint az ügyfelek által kitöltendő kérelmek, nyomtatványok hátoldalán kell feltüntetni, és az Önkormányzat honlapjára fel kell tölteni.

IX. Adatvédelmi hatásvizsgálat

63.§ (1) Az adatvédelmi hatásvizsgálatot a GDPR 35. és 36. cikke alapján az adatvédelmi tisztviselő irányításával munkacsoport végzi, melynek tagjai az adatvédelmi tisztviselő, az informatikai osztály vezetője vagy az általa kijelölt munkatárs, az érintett belső szervezeti egység vezetője vagy a vezető által kijelölt munkatárs.

(2) Adatvédelmi hatásvizsgálat elvégzésére van szükség, ha olyan új technológia, program, rendszer, alkalmazás vagy olyan új eszköz használata kerül bevezetésre, amely személyes adatokat kezel vagy alkalmas ezek kezelésére.

(3) Az adatvédelmi hatásvizsgálat tartalmazza:

a) az adatkezelés bemutatását, ennek körében különösen a kezelt személyes adatok körét, a személyes adatok kezelésének célját, jogalapját, a tárolás időtartamát, a címzetteket és azokat a személyeket, akik az adatokhoz hozzáférhetnek;

b) az adatkezelés folyamatát az adatgyűjtéstől az adatok megsemmisítéséig;

c) az adatkezeléshez kapcsolódó felelősségi viszonyokat;

d) a személyes adatok kezelésére szolgáló eszközöket

e) annak bemutatását, hogy a gyűjtött adatok az adatkezelés céljai szempontjából megfelelőek és relevánsak, a szükségesre korlátozódnak

f) adatminőséget biztosító intézkedéseket

g) azt, hogy az érintetteket milyen módon tájékoztatják az adatkezelésről;

h) a hozzájáruláson alapuló adatkezelés esetében azt, hogy a hozzájárulást az érintettől milyen módon szerzik be, a hozzájárulások nyilvántartása milyen módon történik, azok visszakereshetőségének biztosítását;

i) hogyan biztosítják az érintetti jogokat, így különösen a hozzáférés, adathordozhatóság, helyesbítés, törlés, korlátozás, tiltakozás jogát

j) adatfeldolgozó részére milyen körben, milyen módon, célból, jogalappal történik a személyes adatok továbbítása, adatfeldolgozói kötelezettségeket, adatkezelő ellenőrzési kötelezettségét, jogosultságát;

k) az Európai Unión kívülre történő adattovábbítás esetén az érintett országok megnevezését, továbbá, hogy az adatkezelés és - tárolás megfelelő védelmi szintje biztosított-e;

l) Európai Unión belüli adattovábbítás leírását az adatkezelésre vonatkozó szabályok szerint;

m) adatvédelmi incidens elkerülése, illetve annak megvalósulása esetén annak kezelése érdekében tervezett intézkedéseket, amelyek hozzájárulnak az adatbiztonság megteremtéséhez;

n) adatkezelési kockázatok – adatokhoz való jogosulatlan hozzáférés, adatok véletlen vagy jogellenes megváltoztatása, adatvesztés - feltérképezését a kockázat súlyossága és a bekövetkezésének valószínűsége alapján;

o) az adatvédelmi tisztviselő véleményét;

p) Az adatvédelmi hatásvizsgálat 1 példányát az érintett belső szervezeti egységnél, 1 példányt az adatvédelmi tisztviselőnél kell az iratkezelés szabályai szerint őrizni.

(4) A vizsgálat jelentéssel zárul, amely nem nyilvános.

X. Adatvédelmi incidens kezelése

64.§ (1) Adatvédelmi incidens észlelése esetén a foglalkoztatott kötelessége a belső szervezeti egysége vezetőjét haladéktalanul, de legkésőbb 1 munkaórán belül tájékoztatni az incidensről.

(2) A vezető, az aljegyző a tudomására jutott adatvédelmi incidensről tájékoztatja egyidejűleg a jegyzőt, az adatvédelmi tisztviselőt és informatikai adatbiztonság vélhető sérülése esetén az Informatikai Osztály vezetőjét, függetlenül attól, hogy az adatvédelmi incidens ügyfél által történt bejelentés, adatfeldolgozói tevékenységgel összefüggő feladat ellátás során vagy saját munkakörben történt észlelés során jutott a belső szervezeti egység tudomására.

(3) A tájékoztatásnak tartalmaznia kell:

a) az incidens (észlelt esemény) leírását,

b) az incidens észlelésének időpontját,

c) az érintettek körét,

d) amennyiben megbecsülhető, az érintettek hozzávetőleges számát.

(4) Az adatvédelmi incidensről szóló tájékoztatást az adatvedelem@zuglo.hu és a jegyzo@zuglo.hu email címre, továbbá informatikai adatbiztonság vélhető sérülése esetén az Informatikai Osztály vezetőjének email címére kell megküldeni.

(5) A tájékoztatással egy időben az incidens elhárítása érdekében szükséges és megfelelő intézkedéseket is meg kell tenni.

65.§ (1) Az adatvédelmi incidenst az adatvédelmi tisztviselő indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, bejelenti a NAIH által e célra biztosított elektronikus felületen, kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Ha a bejelentés nem történik meg 72 órán belül, mellékelni kell hozzá a késedelem igazolására szolgáló indokokat is.

(2) Tudomásszerzésnek az az időpont tekinthető, amikor az adatkezelő ésszerű mértékű bizonyossággal rendelkezik arról, hogy olyan biztonsági esemény történt, amely személyes adatokkal kapcsolatos jogellenes műveletekhez vezethet.

66.§ Annak eldöntése, hogy az adatvédelmi incidens kockázati szintje, az eset összes körülményeit és az alkalmazott adatbiztonsági intézkedéseket figyelembe véve miként minősül, az 63. § (1) bekezdés szerinti munkacsoport feladata, melynek összehívását az adatvédelmi tisztviselő kezdeményezi. Sürgős esetben elektronikus úton történő kommunikáció is megengedett.

67.§ Az adatvédelmi tisztviselő, az érintett belső szervezeti egység vezetője és szükség esetén az Informatikai Osztály vezetője vagy az általa kijelölt munkatárs feltárja az adatvédelmi incidens okait, az incidens bekövetkezésének időpontját, az incidenssel érintett személyes adatok körét, az érintettek körét és számát. Amennyiben az érintettek száma nem határozható meg pontosan, akkor a hozzávetőleges számát.

68.§ Az adatvédelmi incidensről - a GDPR-ban előírt esetben - a jegyző tájékoztatja az érintettet. A tájékoztatási kötelezettség jelzése és a tájékoztatás előkészítése az adatvédelmi tisztviselő és az informatikai vezető vagy munkatárs feladata.

69.§ (1) Az adatvédelmi incidens kivizsgálásának eredménye alapján az adatvédelmi tisztviselő, az érintett belső szervezeti egység vezetője és az informatikai adatbiztonság sérülése esetén az Informatikai Osztály vezetője intézkedési terv javaslatot készít a jegyző részére.

(2) Az intézkedési tervben a jegyző meghatározza:

a) az adatvédelmi incidens orvoslására teendő intézkedéseket, beleértve az incidensből eredő hátrányos következmények enyhítését,

b) a jövőbeni incidensek elkerülése érdekében teendő intézkedéseket és

c) feladatok végrehajtásának határidejét, felelősét.

(3) Az intézkedési terv végrehajtásáról a felelősök írásban beszámolnak a jegyzőnek a határidő elteltének napján. A végrehajtásról szóló beszámoló másolatát egyidejűleg meg kell küldeni az adatvédelmi tisztviselő részére.

70.§ (1) Az adatvédelmi tisztviselő a vizsgálatot folyamatosan dokumentálja.

(2) Az adatvédelmi incidenseket, az incidens feltárását rögzítő dokumentumokat, az intézkedési tervet, annak végrehajtásáról szóló beszámolót az adatvédelmi tisztviselő nyilvántartja. A dokumentálásban az incidens kezelésének felelősei kötelesek együttműködni.

XI. Az adatvédelem szervezete

15. Az adatvédelmi tisztviselő feladatai

71.§ § (1) Az adatvédelmi tisztviselő ebben a beosztásában közvetlenül a jegyző alá tartozik, a szervezeti egységet tekintve pedig az Igazgatási és Hatósági Főosztályhoz tagozódik be.

(2) Az adatvédelmi tisztviselő

a) figyelemmel kíséri és értelmezi az információs önrendelkezést, a személyes adatokat, a közérdekű és közérdekből nyilvános adatokat érintő jogszabályokat és állásfoglalásokat, azokat a Hivatal és az Önkormányzat tevékenységének folyamataira alkalmazza;

b) javaslatot tesz az adatvédelemmel összefüggő belső szabályozórendszerre, elkészíti és folyamatos aktualizálja az adatvédelmi és adatbiztonsági szabályzatot, azt a kapcsolódó dokumentumokkal összehangolja;

c) közreműködik, illetőleg segítséget nyújt az adatkezeléssel összefüggő döntések meghozatalában, valamint az érintettek jogainak biztosításában;

d) ellenőrzi az adatkezelésre vonatkozó jogszabályok és szabályzatok rendelkezéseinek betartását, az adatbiztonsági követelmények érvényesülését mind a papír alapú, mind az elektronikus eljárások során;

e) ellenőrzi a kötelezően közzéteendő közérdekű adatok publikálásának teljesítését, szükség szerint intézkedést kezdeményez;

f) kivizsgálja a tárgyban a Hivatalhoz érkezett bejelentéseket, jogosulatlan adatkezelés észlelése esetén annak megszüntetésére hívja fel az adatkezelőt vagy adatfeldolgozót;

g) panasz esetén, illetve hivatalból vizsgálatot kezdeményez az adatkezelésre, az érintettek jogai érvényesülésére, valamint a közérdekű adatok közzétételére vonatkozó rendelkezések betartása érdekében;

h) tájékoztatást nyújt az adatvédelmi ismeretekről;

i) részt vesz a belső kontrollrendszer folyamatok kialakításában, módosításában az adatvédelem célkitűzéseinek megvalósítása érdekében;

j) részt vesz az informatikai biztonság megfelelő szintjének elérése és fenntartása érdekében az informatikai rendszerek kialakítására és üzemeltetésére vonatkozó követelmények meghatározásában, a rendszerek életciklusának folyamatában;

k) az éves statisztikai adatszolgáltatás elkészítésében együttműködik a Jogi Főosztállyal, majd a statisztikai adatokat továbbítja a NAIH részére;

l) állásfoglalásával, javaslatával közreműködik a közérdekű adatigénylések megválaszolásában;

m) közreműködik az adatvédelmi hatásvizsgálat elvégzésében;

n) az adatvédelmi incidens eseményét, a körülmények feltárását, a megtett intézkedéseket dokumentálja, jogszabályban előírt esetben a NAIH részére szolgáló tájékoztatót elkészíti;

o) évente általános adatvédelmi oktatást, szükség esetén eseti oktatást tart a foglalkoztatottak részére, az oktatásokat dokumentálja;

p) vezeti az adatkezelési nyilvántartást, az adatvédelmi incidensekkel kapcsolatban megtett intézkedésekről szóló nyilvántartást, a személyes adatok védelmével kapcsolatosan hozzá érkezett panaszokról, bejelentésekről szóló nyilvántartást, a közérdekű adatok nyilvánosságával kapcsolatosan hozzá érkezett panaszokról, bejelentésekről szóló nyilvántartást.

16. A foglalkoztatottak kötelezettségei

72.§ A Hivatal valamennyi foglalkoztatottja köteles

a) az adatvédelmi előírásokat megismerni, és maradéktalanul betartani, a Szabályzat megismerését az 1. melléklet szerinti megismerési záradékon aláírásukkal igazolni;

b) előzetesen egyeztetni az adatvédelmi tisztviselővel a személyes adatok kezelését vagy a közérdekű adatok nyilvánosságát érintő ügyekben, továbbá a NAIH közreműködését igénylő kérdésekben;

c) a hozzá érkező adatigénylési kérelmekről, bejelentésekről tájékoztatni az adatvédelmi tisztviselőt az adatvedelem@zuglo.hu címen

d) tájékoztatni az adatvédelmi tisztviselőt a felmerült adatvédelmi visszásságról;

e) az adatvédelmi tisztviselő észrevétele esetén az adatkezeléssel kapcsolatosan feltárt visszásságot haladéktalanul megszüntetni;

f) adatokat, iratokat az adatvédelmi tisztviselő kérésére adatvédelmi vizsgálathoz, hatásvizsgálathoz, incidenskezeléshez átadni, mely során felelősséggel tartozik a személyes adatokat tartalmazó dokumentumok teljes körűségéért.

XII. Záró rendelkezések

73.§ (1) Ez az utasítás 2023. június 1. napján lép hatályba.

(2) Hatályát veszti Budapest Főváros XIV. Kerület Zuglói Polgármesteri Hivatal Jegyzőjének Budapest Főváros XIV. Kerület Zuglói Polgármesteri Hivatal Adatvédelmi és Adatbiztonsági Szabályzatáról szóló 12/2018. (VI. 30.) normatív utasítása.

(3) Az utasítás előkészítéséért és aktualizálásáért az adatvédelmi tisztviselő felelős.

Horváth Csaba
polgármester

dr. Tiba Zsolt
jegyző

MEGISMERÉSI ZÁRADÉK

Aláírásommal igazolom, hogy a Szabályzatot elolvastam, annak tartalmát megértettem.

szervezeti egység	név, beosztás	aláírás	dátum