Ikt.sz.: E/1878-1/2026.

Ercsi Város Önkormányzat és Intézményei, valamint
Nemzetiségi Önkormányzatai

ADATVÉDELMI ÉS ADATBIZTONSÁGI KÖZÖS SZABÁLYZAT

Érvényes: 2026. február 15. napjától

Tartalomjegyzék

I. Bevezető 3

II. Általános adatvédelmi szabályok 3

1. A Szabályzat hatálya 3
2. A Szabályzat célja 4
3. Az adatkezelés során használt fontosabb fogalmak 4
4. Az adatkezelés alapelvei 7
5. Személyes adatok védelme 8

III. A polgárok személyes adataival kapcsolatos feladatok és eljárások 9

1. Értelmező rendelkezések 9
2. Adatszolgáltatás (Hozzáférési jog gyakorlása) 10
3. Adatvédelmi tisztviselő 10
4. Adatkezelési nyilvántartás 11
5. Adatvédelmi incidensek 11

IV. Számítástechnikai védelmi szabályok 12

1. Adatok és programok védelme 12
2. Számítógépek, eszközök és dokumentációk védelme 14
3. Mágneses adathordozók védelme 14
4. Az adathordozók selejtezése 15
5. Vírusvédelmi eljárások 15
6. A vírusvédelem szabályai a felhasználó részéről 16
7. Az elektronikus levelezés vírusvédelme 16

V. ZÁRÓ RENDELKEZÉSEK 16

I. Bevezető

Az együttműködő szervezetek az adatvédelemmel összefüggő feladataikat és eljárásaikat közös szabályzatban az alábbiak szerint szabályozzák.

Az együttműködő szervezetek:

Ercsi Város Önkormányzat és Intézményei, nevezetesen: Ercsi Város Polgármesteri Hivatal, Ercsi Egészségügyi Központ, Ercsi Szociális Szolgálat, Ercsi Hétszínvirág Óvoda, Ercsi Napfény Óvoda, Ercsi Eötvös József Művelődési Ház és Könyvtár, továbbá nemzetiségi önkormányzatai: Ercsi Horvát Nemzetiségi Önkormányzat, Ercsi Roma Nemzetiségi Önkormányzat (továbbiakban: Önkormányzat és Intézményei, valamint a nemzetiségi önkormányzatok; vagy adott szervezet/szervezet).

Az Önkormányzat és Intézményei által végzett adatkezelés 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 szóló 2016/679 EU rendeletnek (a továbbiakban: Általános Adatvédelmi Rendelet) és az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infó tv.) és jelen szabályzat (továbbiakban: Szabályzat) rendelkezéseinek megfelelően történik.

II. Általános adatvédelmi szabályok

1. A Szabályzat hatálya

A közös Szabályzat célja, hogy a rendelkezéseink figyelembevételével meghatározza az adott szervezetnek a személyes adatok védelmével kapcsolatos általános feladatait és az eljárás rendjét, továbbá az adatbiztonság követelményeinek érvényesülését.

A Szabályzat személyi hatálya kiterjed a közös szabályzatot alkotó szervezetek vezetőire, ügyintézőire, valamint a munkajogviszony keretében foglalkoztatott ügyviteli és fizikai alkalmazottakra, egyéb munkavállalókra. Kiterjed továbbá azokra a személyekre, akik az önkormányzattól kapott megbízásuk alapján jelen közös szabályzat előírt rendelkezéseivel kapcsolatba kerülnek.

A Szabályzat tárgyi hatálya kiterjed a közös szabályzatot alkotó szervezetek tulajdonát képező, továbbá az épület(ek)ben lévő:

a) valamennyi használatban lévő, vagy tárolt informatikai berendezésre és azok műszaki dokumentációjára függetlenül attól, hogy az személyi használatban vagy szervezeti egység használatában van;
b) adott szervezetnél keletkezett minden elektronikus adatra, annak keletkezésének, felhasználásának és feldolgozásának helyétől és megjelenési formájától függetlenül;
c) valamennyi adathordozóra, azok tárolására és felhasználására, illetve a beérkezés és a feldolgozás közötti időszakra;
d) adott szervezet által használt felhasználói programokra és rendszerprogramokra;
e) az informatikai rendszerben megjelenő valamennyi dokumentációra (fejlesztési, szervezési, programozási, üzemeltetési).

2. A Szabályzat célja

A Szabályzat az informatikai rendszerrel kapcsolatos, biztonságos adatkezelési és adatvédelemi eljárásokat és feladatokat rögzít. A számítástechnikai eszközök beszerzésének és használatának, a saját fejlesztésű, valamint a vásárolt szoftverek alkalmazásának folyamatát, továbbá egyes személyek informatikai biztonságot érintő feladatait.

A személyes adatok védelméért, az adatkezelés jogszerűségéért a szervezet vezetője a felelős. A szervezet által vezetett személyes adatokat tartalmazó, illetve a személyes adatokat nem tartalmazó nyilvántartásokat, valamint az azokból történt adattovábbításokat, továbbá a szervezet által elérhető személyes adatokat tartalmazó, jelen szabályzat **1-6.** számú melléklete tartalmazza.

A szervezetnél nyilvántartott adatokat védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, nyilvánosságra hozatal, illetve a sérülés, törlés, vagy megsemmisülés ellen.

Iratot munkaköri feladat ellátásán kívül a munkahelyről kivinni, valamint munkahelyen kívül feldolgozni, tárolni csak a szervezet vezetője (jegyző) egyetértésével lehet, azzal a feltétellel, hogy az irat tartalmát illetéktelen személy ne ismerje meg.

Az iratok kezelése, tárolása során ki kell zárni annak a lehetőségét, hogy illetéktelen személy az iratok tartalmába betekintést nyerjen. Az iratokat a szervezetnél zárható helységben, elkülönítetten kell tárolni. A munkavégzés céljára szolgáló irodákat a köztisztviselő, munkavállaló távozásakor kulcsra kell zárni.

Az irodahelységek zárásának elmulasztásából eredően az iratokhoz történő illetéktelen hozzáférés esetén az érintett fegyelmi és kártérítési felelősséggel tartozik.

3. Az adatkezelés során használt fontosabb fogalmak

1) *érintett:* bármely információ alapján azonosított vagy azonosítható természetes személy;
2) *azonosítható természetes személy:* az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, azonosító szám, helymeghatározó adat, online azonosító vagy a természetes személy fizikai, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható;
3) *személyes adat:* az érintettre vonatkozó bármely információ;
4) *különleges adat:* a személyes adatok különleges kategóriáiba tartozó minden adat, azaz a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a genetikai adatok, a természetes személyek egyedi azonosítását célzó biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok,
5) *genetikai adat:* egy természetes személy örökölt vagy szerzett genetikai jellemzőire vonatkozó minden olyan személyes adat, amely az adott személy fiziológiájára vagy egészségi állapotára vonatkozó egyedi információt hordoz, és amely elsősorban az adott természetes személyből vett biológiai minta elemzéséből ered;
6) *biometrikus adat:* egy természetes személy fizikai, fiziológiai vagy viselkedési jellemzőire vonatkozó olyan, sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy

megerősíti a természetes személy egyedi azonosítását, mint például az arckép vagy a daktiloszkópiai adat;

7) *egészségügyi adat:* egy természetes személy testi vagy szellemi egészségi állapotára vonatkozó személyes adat, ideértve a természetes személy számára nyújtott egészségügyi szolgáltatásokra vonatkozó olyan adatot is, amely információt hordoz a természetes személy egészségi állapotáról;
8) *bűnügyi személyes adat:* a büntetőeljárás során vagy azt megelőzően a bűncselekménnyel vagy a büntetőeljárással összefüggésben, a büntetőeljárás lefolytatására, illetve a bűncselekmények felderítésére jogosult szerveknél, továbbá a büntetés-végrehajtás szervezeténél keletkezett, az érintettel kapcsolatba hozható, valamint a büntetett előéletre vonatkozó személyes adat;
9) *közérdekű adat:* az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy azt átvevő szerv, szervezet vagy személy (a továbbiakban együtt: közfeladatot ellátó szerv) 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;
10) *közérdekből nyilvános adat:* a közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli;
11) *hozzájárulás:* az érintett akaratának önkéntes, határozott és megfelelő tájékoztatáson alapuló egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy az akaratát félreérthetetlenül kifejező más magatartás útján jelzi, hogy beleegyezését adja a rá vonatkozó személyes adatok kezeléséhez;
12) *adatkezelő:* az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely – törvényben vagy az Európai Unió kötelező jogi aktusában meghatározott keretek között – önállóan vagy másokkal együtt az adat kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja;
13) adatgazda: az adott adatállomány szakmai felelőse (nem azonos az adatkezelővel)
14) *közös adatkezelő:* az az adatkezelő, aki vagy amely – törvényben vagy az Európai Unió kötelező jogi aktusában meghatározott keretek között – az adatkezelés céljait és eszközeit egy vagy több másik adatkezelővel közösen határozza meg, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket egy vagy több másik adatkezelővel közösen hozza meg és hajtja végre vagy hajtatja végre az adatfeldolgozóval;
15) *adatkezelés:* az alkalmazott eljárástól függetlenül az adaton végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adat további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése;

16) *bűnüldözési célú adatkezelés:* a jogszabályban meghatározott feladat- és hatáskörében a közrendet vagy a közbiztonságot fenyegető veszélyek megelőzésére vagy elhárítására, a bűnmegelőzésre, a bűnfelderítésre, a büntetőeljárás lefolytatására vagy ezen eljárásban való közreműködésre, a szabálysértések megelőzésére és felderítésére, valamint a szabálysértési eljárás lefolytatására vagy ezen eljárásban való közreműködésre, továbbá a büntetőeljárásban vagy szabálysértési eljárásban megállapított jogkövetkezmények végrehajtására irányuló tevékenységet folytató szerv vagy személy (a továbbiakban együtt: bűnüldözési adatkezelést folytató szerv) ezen tevékenység keretei között és céljából – ideértve az ezen tevékenységhez kapcsolódó személyes adatok levéltári, tudományos, statisztikai vagy történelmi célból történő kezelését is – (a továbbiakban együtt: bűnüldözési cél) végzett adatkezelése;
17) *nemzetbiztonsági célú adatkezelés:* a nemzetbiztonsági szolgálatok jogszabályban meghatározott feladat- és hatáskörében végzett adatkezelése, valamint a rendőrség terrorizmust elhárító szervének jogszabályban meghatározott feladat- és hatáskörében végzett, a nemzetbiztonsági szolgálatokról szóló törvény hatálya alá tartozó adatkezelése;
18) *honvédelmi célú adatkezelés:* a honvédelmi adatkezelésekről szóló törvény, és a Magyar Köztársaság területén szolgálati céllal tartózkodó külföldi fegyveres erők, valamint a Magyar Köztársaság területén felállított nemzetközi katonai parancsnokságok és állományuk nyilvántartásáról, valamint jogállásukhoz kapcsolódó egyes rendelkezésekről szóló törvény hatálya alá tartozó adatkezelés;
19) *adattovábbítás:* az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele;
20) *közvetett adattovábbítás*: személyes adatnak valamely harmadik országban vagy nemzetközi szervezet keretében adatkezelést folytató adatkezelő vagy adatfeldolgozó részére továbbítása útján valamely más harmadik országban vagy nemzetközi szervezet keretében adatkezelést folytató adatkezelő vagy adatfeldolgozó részére történő továbbítása;
21) *nemzetközi szervezet*: a nemzetközi közjog hatálya alá tartozó szervezet és annak alárendelt szervei, továbbá olyan egyéb szerv, amelyet két vagy több állam közötti megállapodás hozott létre vagy amely ilyen megállapodás alapján jött létre;
22) *nyilvánosságra hozatal:* az adat bárki számára történő hozzáférhetővé tétele;
23) *adattörlés:* az adat felismerhetetlenné tétele oly módon, hogy a helyreállítása többé nem lehetséges;
24) *adatkezelés korlátozása*: a tárolt adat zárolása az adat további kezelésének korlátozása céljából történő megjelölése útján;
25) *adatmegsemmisítés:* az adatot tartalmazó adathordozó teljes fizikai megsemmisítése;
26) *adatfeldolgozás*: az adatkezelő megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által végzett adatkezelési műveletek összessége;
27) *adatfeldolgozó:* az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely – törvényben vagy az Európai Unió kötelező jogi aktusában meghatározott keretek között és feltételekkel – az adatkezelő megbízásából vagy rendelkezése alapján személyes adatokat kezel;
28) *adatfelelős:* az a közfeladatot ellátó szerv, amely az elektronikus úton kötelezően közzéteendő közérdekű adatot előállította, illetve amelynek a működése során ez az adat keletkezett;
29) *adatközlő:* az a közfeladatot ellátó szerv, amely – ha az adatfelelős nem maga teszi közzé az adatot – az adatfelelős által hozzá eljuttatott adatot honlapon közzéteszi;
30) *adatállomány:* az egy nyilvántartásban kezelt adatok összessége;

31) *harmadik személy:* olyan természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely nem azonos az érintettel, az adatkezelővel, az adatfeldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére irányuló műveleteket végeznek;
32) *EGT-állam:* az Európai Unió tagállama és az Európai Gazdasági Térségről szóló megállapodásban részes más állam, továbbá az az állam, amelynek állampolgára az Európai Unió és tagállamai, valamint az Európai Gazdasági Térségről szóló megállapodásban nem részes állam között létrejött nemzetközi szerződés alapján az Európai Gazdasági Térségről szóló megállapodásban részes állam állampolgárával azonos jogállást élvez;
33) *harmadik ország:* minden olyan állam, amely nem EGT-állam;
34) *adatvédelmi incidens:* az adatbiztonság olyan sérelme, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisülését, elvesztését, módosulását, jogosulatlan továbbítását vagy nyilvánosságra hozatalát, vagy az azokhoz való jogosulatlan hozzáférést eredményezi;
35) *profilalkotás:* személyes adat bármely olyan – automatizált módon történő – kezelése, amely az érintett személyes jellemzőinek, különösen a munkahelyi teljesítményéhez, gazdasági helyzetéhez, egészségi állapotához, személyes preferenciáihoz vagy érdeklődéséhez, megbízhatóságához, viselkedéséhez, tartózkodási helyéhez vagy mozgásához kapcsolódó jellemzőinek értékelésére, elemzésére vagy előrejelzésére irányul;
36) *címzett:* az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely részére személyes adatot az adatkezelő, illetve az adatfeldolgozó hozzáférhetővé tesz;
37) *álnevesítés:* személyes adat olyan módon történő kezelése, amely – a személyes adattól elkülönítve tárolt – további információ felhasználása nélkül megállapíthatatlanná teszi, hogy a személyes adat mely érintettre vonatkozik, valamint műszaki és szervezési intézkedések megtételével biztosítja, hogy azt azonosított vagy azonosítható természetes személyhez ne lehessen kapcsolni;

4. Az adatkezelés alapelvei

A személyes adatok kezelésének megkezdése előtt az adatkezelő Önkormányzat és Intézményei, minden esetben gondosan mérlegelik hogy ténylegesen szükséges-e az adatok kezelése az adatkezelés céljának elérése érdekében. Személyes adatok kezelését kizárólag akkor lehet megkezdeni, ha kétséget kizáróan indokolható, hogy az adatkezelés célját más módon nem lehet megvalósítani.

Az Önkormányzat és Intézményei, kötelesek az érintettek személyes adatait jogszerűen, tisztességesen, átlátható módon kezelni.

Az érintettek személyes adatainak gyűjtése csak meghatározott, egyértelmű és jogszerű célból történhet. Az Önkormányzat és Intézményei, kötelesek eleve elkerülni, illetve utóbb megszüntetni minden olyan adatkezelés, amely az adott személyes adatra vonatkozó céllal össze nem egyeztethető módon történik. Az Önkormányzat és Intézményei csak a szükséges mértékben

jogosultak személyes adatot kezelni, és kötelesek minden olyan személyes adatot törölni, amelynek tekintetében az adatkezelés célja megszűnt, illetve az adatkezelés jogalapja nem igazolható.

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

Az Önkormányzat és Intézményei, kötelesek olyan kontrollmechanizmusokat bevezetni, amelyek alkalmasak arra, hogy már előzetesen is, illetve utóbb szűrő jelleggel biztosítható legyen, hogy

a) a személyes adatok már az adatfelvétel időpontjában, majd az adatkezelés teljes időtartama alatt az adatkezelés céljainak megfelelnek, továbbá

b) az adatkezelés mértéke mind az adatok körét, mind az adatkezelés időtartamát illetően a szükségesre korlátozódik.

Az Önkormányzat és Intézményei által kezelt személyes adatoknak pontosnak és naprakésznek kell lenniük.

A személyes adatok tárolásának olyan formában kell történnie, amely az Érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé.

A személyes adatok kezelését olyan módon kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, ideértve mindazon lepéseket, melyek a személyes adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmét szolgálja.

5. Személyes adatok védelme

A szervezet vezetője a személyes adatok kezelését végző személy munkaköri leírásában határozza meg az általa kezelhető és elérhető nyilvántartások körét. A személyes adatok kezelését végző személy felelősséggel tartozik azért, hogy tevékenységét az adatkezelésre és az adatok védelmére vonatkozó jogszabályoknak megfelelően végezze.

Az adatkezelési tevékenységet végző személyek kötelesek az adatvédelmi és az adatbiztonsági szabályokat betartani.

Az adatgazda azokat a személyes adatokat kezelheti, illetve veheti át harmadik személytől, amelyek kezelésére törvény vagy az érintett felhatalmazza.

Az adatok tárolási módját úgy kell megválasztani, hogy törlésük az adattörlési határidő lejártakor, illetve, ha az más okból szükséges, elvégezhető legyen.

A szervezet számítógépes hálózatán lévő nyilvántartásokba történő belépés a szervezet vezetőjének döntése alapján — a személyes jelszón kívül — a hálózati szoftverben egyedileg

előállított hozzáféréssel engedélyezhető. A belépés csak a legszükségesebb körben, az ügyintéző munkaköri feladatai ellátásához kapcsolódóan engedélyezhető a következők szerint:

Megnevezés	Hozzáférési jogosultság
Ügyirat nyilvántartás	ügyiratkezelők
Közszolgálati alapnyilvántartás KÖZIGTAD	személyzeti ügyintéző
Illetmény átutalás	pénzügyi ügyintéző
Hatósági statisztika	hatósági ügyintéző
Szabálysértési statisztika	hatósági ügyintéző
Gyámügyi statisztika	gyámügyi ügyintéző
Vagyonnyilvántartás	pénzügyi ügyintéző

A szervezet által elérhető nem saját személyes adatokat tartalmazó nyilvántartásokból történő adatkezelés esetén az alábbiak szerint kell eljárni:

a) Az adatkezelésre jogosultak névsorának jóváhagyása a szervezet vezetője (jegyző) feladatkörébe tartozik. A belépésre vonatkozó személyi javaslat csak a munkavégzéshez feltétlenül szükséges, lehető legszűkebb körre vonatkozhat.
b) A nyilvántartási rendszerekhez hozzáférési jogosultsággal rendelkezők névsorát az informatikus köteles naprakészen vezetni.
c) Hozzáférési jogosultsággal rendelkező adatgazda az adat lekérdezésekről a Szabályzat **8.** számú mellékletét képező „Adatszolgáltatási nyilvántartást" köteles vezetni.

III. A polgárok személyes adataival kapcsolatos feladatok és eljárások

1. Értelmező rendelkezések

A polgár természetes személyazonosító adatai:

d) családi és utóneve, továbbá születéskori családi és utóneve (a továbbiakban együtt: név);
e) neme;
f) születési helye és ideje;
g) anyja születéskori családi és utóneve(i) (a továbbiakban: anyja neve).

A polgár lakcím adata: bejelentett lakóhelyének, illetve tartózkodási helyének címe (a továbbiakban együtt: lakcím).

Adatszolgáltatás: a nyilvántartásban szereplő polgárok személyes adatainak az adatvédelmin jogszabályokban meghatározott tartalmú és terjedelmű közlése. Ezen belül:

a) egyedi adatszolgáltatás: egy polgár adatainak közlése;
b) csoportos adatszolgáltatás: az adatigénylő által vagy jogszabályban meghatározott szempontok szerint képzett csoportba tartozó polgárok adatainak rendszeres vagy eseti közlése.

2. Adatszolgáltatás (Hozzáférési jog gyakorlása)

Az érintett jogosult arra, hogy az adatkezelő Önkormányzat és Intézményei elérhetőségein tájékoztatást kérjen arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e, és ha ilyen adatkezelés folyamatban van, jogosult arra, hogy megismerje azt, hogy az adatkezelő:

a) milyen személyes adatait, milyen jogalapon, milyen adatkezelési célból, illetve mennyi ideig kezeli;
b) kinek, mikor, milyen jogszabály alapján, mely személyes adataihoz biztosított hozzáférést vagy kinek továbbította a személyes adatait; milyen forrásból származnak a személyes adatai;
c) alkalmaz-e automatizált döntéshozatalt, és ha igen, jogosult megismerni annak logikáját, ideértve a profilalkotást is.

Az Önkormányzat és Intézményei az adatkezelés tárgyat képező személyes adatok másolatát az érintett erre irányuló kérésére első alkalommal díjmentesen bocsátja a rendelkezésére, ezt követően az Általános Adatvédelmi Rendelet 12. cikk (5) bekezdésével összhangban, ha az érintett kérelme egyértelműen megalapozatlan, vagy – különösen ismétlődő jellege miatt – túlzó, adminisztratív költségeken alapuló, ésszerű mértékű díjat számíthat fel, vagy megtagadhatja a kérelem alapján történő intézkedést.

Az adatkezelő az Általános Adatvédelmi Rendelet 12. cikk (3) bekezdésével összhangban, az érintett jogai gyakorlására irányuló kérelmét indokolatlan késedelem nélkül, de legfeljebb az annak beérkezésétől számított egy hónapon belül teljesíti. Szükség esetén, figyelembe véve a kérelem bonyolultságát és a beérkezett kérelmek számát, ez a határidő további két hónappal meghosszabbítható. A határidő meghosszabbításáról az Önkormányzat és Intézményei a késedelem okainak megjelölésével a kérelem kézhezvételétől számított egy hónapon belül tájékoztatják az érintettet.

Az adatszolgáltatás iránti kérelem elbírálása az adott szervezet vezetőjének hatáskörébe tartozik.

Adatszolgáltatásnak minősül, így a nyilvántartásnak tartalmaznia kell a szervezet munkatársai által, feladatkörük ellátása érdekében, egyedi ügyeik elintézése céljából igényelt adatok közlését is.

Az érintett személy adatai szolgáltatását korlátozó, vagy tiltó nyilatkozatát (**10. sz. melléklet**), illetőleg annak visszavonását személyesen, vagy meghatalmazott képviselője útján, továbbá ajánlott levélben teheti meg a szervezetnél. A szervezet vezetője által kijelölt személy köteles az adatszolgáltatást korlátozó, vagy megtiltó, vagy ezek visszavonásáról rendelkező nyilatkozatokról nyilvántartást vezetni (**9. sz. melléklet**). Az érintett személy, tájékoztatást kérhet személyes adatai kezeléséről, kérheti személyes adatainak helyesbítését vagy törlését.

3. Adatvédelmi tisztviselő

Az Önkormányzat és Intézményei, mint adatkezelők, jogszabályban rögzített adatvédelmi feladataik ellátására, valamint az adatvédelmi tudatosság elősegítése érdekében adatvédelmi tisztviselőt jelölnek ki.

Az adatkezelő időben bevonja az adatvédelmi tisztviselőt valamennyi, a személyes adatok védelmét érintő döntés előkészítésébe, továbbá biztosítja az adatvédelmi tisztviselő számára mindazon feltételeket, jogosultságokat és erőforrásokat, továbbá hozzáférést biztosít mindazon adatokhoz és

információkhoz, amelyek az adatvédelmi tisztviselő által ellátandó feladatok végrehajtásához, valamint az adatvédelmi tisztviselő szakmai ismereteinek naprakészen tartásához szükségesek.

Az adatvédelmi tisztviselő elősegíti az adatkezelő, illetve az adatfeldolgozó – a személyes adatok kezelésére vonatkozó jogi előírásokban meghatározott – kötelezettségeinek teljesítését, így különösen:

a) a személyes adatok kezelésére vonatkozó jogi előírásokról naprakész tájékoztatást nyújt és azok érvényesítésének módjaival kapcsolatban tanácsot ad az adatkezelő, valamint az adatkezelési műveleteket végző személyek részére;
b) folyamatosan figyelemmel kíséri és ellenőrzi a személyes adatok kezelésére vonatkozó jogi előírások, így különösen a jogszabályok és belső, adatvédelemhez kapcsolódó szabályzatok érvényesülését,
c) elősegíti az érintettet megillető jogok gyakorlását, így különösen kivizsgálja az érintettek panaszait és kezdeményezi az adatkezelőnél, illetve az adatfeldolgozónál a panasz orvoslásához szükséges intézkedések megtételét,
d) szakmai tanácsadással elősegíti és figyelemmel kíséri az adatvédelmi hatásvizsgálat lefolytatását,
e) együttműködik az adatkezelés jogszerűségével kapcsolatos eljárások lefolytatására jogosult szervekkel és személyekkel, így különösen kapcsolatot tart a Hatósággal az előzetes konzultáció és a Hatóság által lefolytatott eljárások elősegítése érdekében,
f) közreműködik a belső adatvédelmi és adatbiztonsági szabályzat megalkotásában.

4. Adatkezelési nyilvántartás

Az adatkezelő Önkormányzat és Intézményei a kezelésében lévő személyes adatokkal kapcsolatos adatkezeléseiről, az adatvédelmi incidensekről és az érintett hozzáférési jogával kapcsolatos intézkedésekről nyilvántartást vezet. Az adatkezelői nyilvántartásban az adatkezelő rögzíti:

g) az adatkezelő, valamint az adatvédelmi tisztviselő nevét és elérhetőségeit,
h) az adatkezelés célját vagy céljait,
i) személyes adatok továbbítása vagy tervezett továbbítása esetén az adattovábbítás címzettjeinek körét,
j) az érintettek, valamint a kezelt adatok körét,
k) profilalkotás alkalmazása esetén annak tényét,
l) nemzetközi adattovábbítás esetén a továbbított adatok körét,
m) az adatkezelési műveletek – ideértve az adattovábbítást is – jogalapjait,
n) ha az ismert, a kezelt személyes adatok törlésének időpontját,
o) az e törvény szerint végrehajtott műszaki és szervezési biztonsági intézkedések általános leírását,
p) az általa kezelt adatokkal összefüggésben felmerült adatvédelmi incidensek bekövetkezésének körülményeit, azok hatásait és a kezelésükre tett intézkedéseket,
q) az érintett hozzáférési jogának érvényesítését e törvény szerint korlátozó vagy megtagadó intézkedésének jogi és ténybeli indokait.

5. Adatvédelmi incidensek

Az adatkezelő Önkormányzat és Intézményei az általuk, illetve a megbízásukból vagy rendelkezése alapján eljáró adatfeldolgozó által kezelt adatokkal összefüggésben felmerült adatvédelmi incidenst

haladéktalanul, de legfeljebb az adatvédelmi incidensről való tudomásszerzését követő 72 órán belül bejelenti a Nemzeti Adatvédelmi és Információszabadság Hatóságnak.

Az adatvédelmi incidenst nem kell bejelenteni, ha valószínűsíthető, hogy az nem jár kockázattal az érintettek jogainak érvényesülésére.

Az adatkezelő a bejelentésben különösen az alábbiakról ad tájékoztatást:

a) ismerteti az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek körét és hozzávetőleges számát, valamint az incidenssel érintett adatok körét és hozzávetőleges mennyiségét,
b) tájékoztatást nyújt az adatvédelmi tisztviselő vagy a további tájékoztatás nyújtására kijelölt más kapcsolattartó nevéről és elérhetőségi adatairól,
c) ismerteti az adatvédelmi incidensből eredő, valószínűsíthető következményeket, és
d) ismerteti az adatkezelő által az adatvédelmi incidens kezelésére tett vagy tervezett – az adatvédelmi incidensből eredő esetleges hátrányos következmények mérséklését célzó és egyéb intézkedéseket.

Amennyiben valamely információ a bejelentés időpontjában nem áll az adatkezelő rendelkezésére, azzal az adatkezelő a bejelentést annak benyújtását követően utólag – az információ rendelkezésre állásáról való tudomásszerzését követően haladéktalanul – kiegészíti.

Ha az adatvédelmi incidens valószínűsíthetően az érintettet megillető valamely alapvető jog érvényesülését lényegesen befolyásoló következményekkel jár, így magas kockázatú, az adatkezelő az érintettet az adatvédelmi incidensről haladéktalanul tájékoztatja.

Az adatkezelő mentesül tájékoztatási kötelezettsége alól, ha

a) az adatkezelő az adatvédelmi incidenssel érintett adatok tekintetében az adatvédelmi incidenst megelőzően megfelelő – így különösen az adatokat a jogosulatlan személy általi hozzáférés esetére értelmezhetetlenné alakító, azok titkosítását eredményező – műszaki és szervezési védelmi intézkedéseket alkalmazott,
   az adatkezelő az adatvédelmi incidensről való tudomásszerzését követően alkalmazott intézkedésekkel biztosította, hogy az adatvédelmi incidens folytán az érintettet megillető valamely alapvető jog érvényesülését lényegesen befolyásoló következmények valószínűsíthetően nem következnek be,
b) az érintett (1) bekezdés szerinti közvetlen tájékoztatása csak az adatkezelő aránytalan erőfeszítésével lenne teljesíthető, ezért az adatkezelő az érintettek részére az adatvédelmi incidenssel összefüggő megfelelő tájékoztatást bárki által hozzáférhető módon közzétett információk útján biztosítja, vagy
c) törvény a tájékoztatást kizárja.

IV. Számítástechnikai védelmi szabályok

1. Adatok és programok védelme

A szervezet számítógépes adatfeldolgozási folyamatai során használt információkat és programokat fokozott biztonsági szabályok szerint kell kezelni. Ennek oka, hogy a számítógépen titoknak minősített adatokat nem tárolnak, illetve a feldolgozás során keletkező adatok sem

minősülnek titkosnak. A fokozatba sorolás független az adatok megjelenési formájától. Ettől eltérő esetben a titkos ügykezelés szabályai szerint kell eljárni.

A szervezetnél működő számítógépeken csak előzetesen ellenőrzött programot szabad futtatni. Az ellenőrzésnek ki kell terjednie a vásárolt vagy átvett program tesztelésére, esetleges működést akadályozó hibák felderítésére. A feltárt hiányosságokról jegyzőkönyvet kell felvenni, melyet a programot szállító szervhez haladéktalanul el kell juttatni. Hibás programot üzembe helyezni tilos.

Tilos vírusellenőrzés nélkül adathordozót a számítógépbe helyezni, arról programot vagy adatot a rendszerbe tölteni.

A tesztelést a felhasználóval közösen az informatikai feladatot ellátó informatikus végzi.

Vásárolt, vagy átvett adathordozón tárolt program esetén minden esetben biztonsági másolatot kell készíteni, majd az eredeti lemezt írásvédetté kell tenni.

A programok felhasználói dokumentációját a felhasználás helyén kell elhelyezni.

Adatok feldolgozásra történő előkészítése:

a) Számítástechnikai feldolgozásra csak tartalmilag és formailag ellenőrzött adatok kerülhetnek.
b) Az ellenőrzésért az adatfelelősség elve szerint adatlapos rögzítés esetén az adatlapot kiállító, adatlap nélküli rögzítés esetén feldolgozást végző kijelölt személy a felelős. Lehetőség szerint biztosítani kell, hogy az adatok a keletkezés helyén kerüljenek rögzítésre.

Feldolgozás folyamata

a) Az adatállományok módosítását kizárólag csak a feldolgozásra készült programmal lehet elvégezni.
b) Az adatfeldolgozás során a számítógép- vagy programhibából adódó adatvesztés fordulhat elő. Ilyenkor az adatrögzítést azonnal be kell fejezni és a további adatvesztés elkerülésére az informatikust haladéktalanul értesíteni kell.

Mentés

A számítógépeken tárolt információk biztonságos megőrzése céljából az adatkezelő Önkormányzat és Intézményei azokról heti rendszerességgel mentést készít és helyi adattároló eszközön (NAS) tárolja.

Másolás

A számítógépes programok a szerzői jog szerint védelmet élvezek, ezért másolásuk, harmadik fél számára történő továbbadásuk tilos.

Törlés

Mágneses adathordozókon tárolt adatok és programok törlését csak a tevékenységet felügyelő illetékes vezető írásbeli engedélye alapján lehet elvégezi. Külön figyelmet kell fordítani az irattározási és selejtezési szabályok betartására.

Visszatöltés

Az adathordozókon tárolt adatok visszatöltését, visszaállítását a szervezetnél annak vezetője engedélyezheti. Ez alól kivételt képeznek az egyedi felhasználók, akik a mentésekből saját munkakönyvtáruk adatait engedély nélkül is visszatöltetik.

Hálózati alkalmazások esetében az adatvesztés elkerülésére és az adatbiztonság fokozására személyre lebontott hozzáférési jogosultságot kell meghatározni (**11. sz.** melléket).

2. Számítógépek, eszközök és dokumentációk védelme

A számítógépek és eszközök rendeltetésszerű használatáért a személyi leltár szerint a használatra kijelölt személy a felelős.

A hálózati működő számítógépeken kizárólag az erre kiképzett szakemberek dolgozhatnak.

Meghibásodás megelőzéséről folyamatos karbantartással kell gondoskodni, üzemzavar esetén a javítást csak arra kiképzett szakember végezheti.

Fizikai sérülések megelőzésére (pl.: hálózati vezetékszakadás) a számítógépet telepítési helyéről elmozdítani, vagy áthelyezni nem szabad.

Vagyonvédelmi megfontolásból azokat a szobákat, ahol számítógép üzemel, biztonsági felszereléssel kell ellátni. A számítógépet használó személy köteles a munkaidő végzetével a számítógépet kikapcsolni, az azok elhelyezésére szolgáló irodahelységet bezárni és a kulcsot az időpont dokumentálásával elzárt helyen letenni. A szervezettől javításra, vagy más célból elszállítani eszközöket csak bizonylatolás után lehet.

Elektromos érintésvédelmi szempontból a számítástechnikai eszközöket csak védőföldeléses, minden számítógéphez leltár szerint tartozó biztonsági kapcsolóval ellátott dugaszoló aljzatba lehet csatlakoztatni. Annak sérülését minden esetben jelezni kell. A berendezéseket vízzel oltani vagy tisztítani tilos.

A tűz elleni védekezés rendjét és elhárítása érdekében szükséges intézkedéseket a szervezet Tűzvédelmi Szabályzata tartalmazza.

3. Mágneses adathordozók védelme

A mágneses adathordozók védelmére és azonosítására az adathordozókat azonosítóval (címkével) kell ellátni és azokról nyilvántartást kell vezetni.

A mentést tartalmazó adathordozók megőrzési idejét úgy kell meghatározni, hogy azokról az aktuális adatállomány sérülés esetén visszaállítható legyen. Vírust tartalmazó, nem mentesíthető adathordozót használatban tartani nem lehet. Az adathordozót óvni kell a szennyeződésektől és a fizikai sérüléstől.

Külső szervnek átadott adathordozókról átadás-átvételi nyilatkozatot (az átadás, átvétel időpontját, az átadás célját, az átadott adathordozó számát, tartalmát az átvevő szerv megnevezését és címét, az átadás idejét, (ideiglenesen vagy véglegesen) az átvevő szerv, őrzéssel megbízott felelősének

megnevezését, valamint az átadó és átvevő szerv erre feljogosított képviselőjének aláírását tartalmazó jegyzéket) kell készíteni.

4. Az adathordozók selejtezése

A szervezet által vásárolt és a dolgozó(k) részére kiadott adathordozót abban az esetben kell selejtezni, ha:

a) fizikailag megsérült,
b) gyári, gyártási hibából következően felhasználásra alkalmatlan,
c) a tároló kapacitás a megengedhető érték alá csökken,
d) véglegesen elhasználódott.

A felhasználók felelőssége, hogy a használhatatlanná vált adathordozókat (CD, DVD, pendrive stb.) a szervezet vezetője felé jelezze, aki gondoskodik azok közös helyen történő összegyűjtéséről. A selejtezés előtt biztosítani kell az adathordozón tárolt adatok biztonságos törlését (fizikai törléssel, formattálással). Ha a tárolt adatok biztonságosan nem törölhetők, akkor az adathordozót úgy kell megsemmisíteni, hogy további felhasználásra már alkalmatlan legyen, azaz fizikai roncsolással kell használhatatlanná tenni.

A megsemmisítés során a felesleges vagyontárgyak hasznosításának és selejtezésének szabályzatában előírtak szerint kell eljárni, annak tényét megsemmisítési jegyzőkönyvben kell rögzíteni.

5. Vírusvédelmi eljárások

A szervezetnél alkalmazott vírusvédelmi rendszernek meg kell felelnie a következő elvárásnak:

a vírusvédelmi szoftvernek, jó minőségűnek és kellő gyakorisággal aktualizáltnak (frissítettnek) kell lennie, hogy felismerési hatékonysága maximális legyen; _ a vírus védelmi szoftvernek minden támadási ponton aktívan üzemelnie kell.

A szervezet egészére kiterjedően a vírusfertőzések megelőzése, kiszűrése és megszüntetése céljából vírusvédelemi szoftvert alkalmaz. A szoftver teljes számítástechnikai gépparkot lefedő (beleértve a mobil eszközöket is) telepítéséért, naprakész és folyamatos üzemeltetéséért, frissítéséért, a vírustámadások elleni védekezés megszervezéséért az informatikus a felelős. Az újonnan vásárolt számítógépekre azok rendszerbe állítása során telepíteni kell a víruskereső programot.

A számítógépes munkaállomásokon a víruskereső programot úgy kell beállítani, hogy naponta egyszer (az első bejelentkezéskor) megtörténjen az automatikus vírusteszt futtatása. A rendszerbe kívülről bekerülő adatokat (USB portról csatlakoztatható eszközök, CD-ROM, Internet stb.) felhasználás előtt vírusellenőrzésnek kell alávetni. A víruskereső program munkaállomásokon történő lefuttatása a felhasználó feladata és felelőssége.

A víruskereső szoftvernek minden lehetséges bejutási pontot (USB portról csatlakoztatható eszközök, CD-ROM, hálózat, e-mail, stb.) ellenőriznie kell, így az elsődleges támadási felületnek

minősülő munkaállomásokat, és a másodlagos támadási felületnek minősülő tűzfalakat, alkalmazás és levelező szervereket.

6. A vírusvédelem szabályai a felhasználó részéről

A szervezetnél alkalmazott vírusvédelmi rendszer a számítógépek működése közben folyamatosan dolgozik, így a felhasználói munka során igénybe vett állományok (programok, adatok, dokumentumok) közvetlenül már a használat előtt vírusellenőrzése kerülnek. A számítástechnikai eszközökön beállított aktív védelemi rendszer kikapcsolása tilos. A rendszer kikapcsolásából adódó károkért (adatvesztés, illetéktelen hozzáférés stb.) a szabályt megszegő teljes körű felelősséggel tartozik.

Amennyiben a felhasználó a víruskereső program „futtatása" során vírust észlel, azonnal jelentenie kell az informatikus felé, aki feljegyezi a vírus és a fertőzött file nevét, továbbá a munkaállomás számát (helyét). Az informatikus gondoskodik a vírus további terjedésének megakadályozásáról, és — amennyiben a felhasználói gépen futó program automatikusan nem törölte — a vírus szakszerű kiirtásáról.

7. Az elektronikus levelezés vírusvédelme

Ha a szervezet elektronikus levelezési rendszerén keresztül fertőzött levél, vagy csatolt állomány érkezik, arról a víruskereső szoftver értesíti a felhasználót (és amennyiben van a rendszergazdát). Ha az aktív védelem a fertőzött állományt eltávolítja, akkor a munka megkezdhető vagy tovább folytatható, amennyiben nem képes a fertőzés eltávolítására, akkor a víruskereső rendszer a fertőzött állományt törli.

Ha a felhasználó levelezési rendszerébe indokolatlan vagy váratlan e-mail érkezik annak tartalmát személyesen (pl. telefonon, e-mailben) ellenőrizni szükséges.

V. ZÁRÓ RENDELKEZÉSEK

A szabályzat 2026. február 15-én lép hatályba.

Adott szervezet vezetőjének kell gondoskodnia, hogy a szabályzatban foglalt előírásokat az érintett munkatársak megismerjék, annak tényét megismerési nyilatkozat aláírásával igazolják.

Ercsi, 2026. február 15.

Jóváhagyta:

Gólics Ildikó
polgármester
Ercsi Város Önkormányzat

Kondrát Zita
jegyző
Ercsi Polgármesteri Hivatal

1. sz. melléklet

Személyes adatokat tartalmazó nyilvántartás

Saját nyilvántartások

Sorszám	Megnevezés	Nyilvántartás típusa	Jogszabályi alap	Érintettek köre	Adatok forrása	Adatkezelés		Archiválás	Adattovábbítás	Adatvédelmi szabályzat	Hozzáférési jogosultság	
						helye	módja				Adatfeldolgozás	csak lekérdezés
1.												
2.												
3.												
4.												
5.												
6.												
7.												
8.												
9.												
10.												
11.												
12.												
13.												
14.												
15.												
16.												
17.												

2. számú melléklet

Személyes adatokat tartalmazó nyilvántartás

Elérhető nem saját nyilvántartások

Sorszám	Megnevezés	Jogszabályi alap	Rendszergaza, üzemeltető	Érintettek köre	Adatkezelés		Adat-továbbítás	Adatvédelmi szabályzat	Hozzáférési jogosultság			
					helye	módja			Engedélyező	Rendelkező	Adatfeldolgozás	csak lekérdezés
1.												
2.												
3.												
4.												
5.												
6.												
7.												
8.												
9.												
10.												
11.												
12.												
13.												
14.												
15.												
16.												
17.												

3. sz. melléklet

Személyes adatokat tartalmazó nyilvántartás

Adattovábbítás

Sorszám	Megnevezés	Nyilvántartás típusa	Jogszabályi alap	Továbbított adatok köre	Adathordozó	Adatküldés módja	Adatküldés gyakorisága	Címzett megnevezése
1.								
2.								
3.								
4.								
5.								
6.								
7.								
8.								
9.								
10.								
11.								
12.								
13.								
14.								
15.								
16.								
17.								

4. sz. melléklet

Személyes adatokat nem tartalmazó nyilvántartás

Saját nyilvántartások

Sorszám	Megnevezés	Nyilvántartás típusa	Jogszabályi alap	Adatok köre	Adatok forrása	Adatkezelés		Archiválás	Adattovábbítás	Adatvédelmi szabályzat	Hozzáférési jogosultság	
						helye	módja				Adatfeldolgozás	csak lekérdezés
1.												
2.												
3.												
4.												
5.												
6.												
7.												
8.												
9.												
10.												
11.												
12.												
13.												
14.												
15.												
16.												
17.												

5. sz. melléklet

Személyes adatokat nem tartalmazó nyilvántartás

Adattovábbítás

Sorszám	Megnevezés	Nyilvántartás típusa	Jogszabályi alap	Továbbított adatok köre	Adathordozó	Adatküldés módja	Adatküldés gyakorisága	Címzett megnevezése
1.								
2.								
3.								
4.								
5.								
6.								
7.								
8.								
9.								
10.								
11.								
12.								
13.								
14.								
15.								
16.								
17.								

6. sz. melléklet

Hozzáférési jogosultság

Sorszám	Adatfeldolgozás megnevezése	Ügyiratszám	Név	Munkáltató megnevezése	Munkakör/beosztás megnevezése
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					
11.					
12.					
13.					
14.					
15.					
16.					
17.					

7. sz. melléklet

A számítógépes rendszerbe belépésre jogosultakról

Sorszám	Belépésre jogosult neve	Munkáltató/intézmény	Munkakör/beosztás megnevezése
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			
11.			
12.			
13.			
14.			
15.			
16.			
17.			
18.			
19.			
20.			
21.			
22.			

8. sz. melléklet

Adatszolgáltatási Nyilvántartás

Adatszolgáltatási ügyintéző neve: _____

Az adatszolgáltatás adatbázisa: _____

Sorszám	Adatszolgáltatás dátuma	Ügyiratszám	Érintett személy neve	Adatigénylő megnevezése	Lekérdezés célja/jogalapja	Lekérdező neve	Megjegyzés
1.							
2.							
3.							
4.							
5.							
6.							
7.							
8.							
9.							
10.							
11.							
12.							
13.							
14.							
15.							
16.							
17.							
18.							
19.							

9. sz. melléklet

Az adatszolgáltatási korlátozásról tett nyilatkozatok nyilvántartása

Sorszám	Nyilatkozó neve	Lakóhelye	Nyilatkozó elérhetősége	Nyilatkozattétel dátuma
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				

10. sz. melléklet

Ercsi Város Önkormányzat
Ercsi
Fő u. 20.
2451

Tárgy: Adatszolgáltatási hozzájárulás megszüntetése

Tisztelt Önkormányzat!

Alulírott, _____ (lakcím: _____)
nem járulok hozzá személyes adataim kiadásához és az erre irányuló adatszolgáltatáshoz.

A fenti hozzájárulás megszüntetésére tekintettel az Önkormányzat által vezetett valamennyi nyilvántartásban vezetett személyes adatom külön-külön is kizárólag írásbeli engedélyem alapján adható ki.

Kérem, hogy a feni nyilatkozat alapján megtett intézkedéséről tájékoztatni szíveskedjen.

Kelt: _____

_____
Nyilatkozó aláírása

11. sz. melléklet

Hozzáférési jogosultság nyilvántartása

Sorszám	Adatfeldolgozás megnevezése	Név	Beosztás/munkakör
1.	Ügyirat nyilvántartás		
2.	Közszolgálati alapnyilvántartás (KÖZIGTAD)		
3.	Illetmény átutalás		
4.	Hatósági statisztika		
5.	Vagyonnyilvántartás		
6.			
7.			
8.			
9.			
10.			

Adatvédelmi és adatbiztonsági szabályzat
Megismerési nyilatkozat

Nyilatkozó neve	Beosztása	Dátum	Aláírás