EGYSÉGES ADATVÉDELMI SZABÁLYZAT
GONDOZÁSI KÖZPONT
SZÁMÁRA

2025.JANUÁR 1

TARTALOMJEGYZÉK

7.2. Manuális kezelésű adatok

MELLÉKLETEK

1. sz. melléklet *Adatvédelmi tájékoztató szöveg a Vecsés Város Önkormányzata által fenntartott intézmények által használt nyomtatványokra*

Preambulum

Vecsés Város Önkormányzata általa fenntartott intézményként

(továbbiakban együttesen: Adatkezelő)

AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE (2016. április 27.) 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 (általános adatvédelmi rendelet),

Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (továbbiakban: Infotv.), valamint

A személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól szóló 2005. évi CXXXIII. törvény,

A digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól szóló 2023. évi CIII. törvény és

Az Európai Parlament és a Tanács 910/2014/EU rendelete (2014. július 23.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról (eIdas Rendelet)

alapján **az intézmény mint adatkezelő**

adatvédelmének, adatbiztonságának és adatkezelésének rendjének szabályozása érdekében az alábbi szabályzatot alkotja.

Az Adatkezelőnél történő személyes adatkezelést további ágazati részletező szabályok is meghatározhatják, amelyeket az Adatkezelő az adatkezelés során szem előtt tart és jelen szabályzat megalkotása során figyelembe vesz.

I. ÁLTALÁNOS RENDELKEZÉSEK

1. A szabályzat célja és hatálya

(1) Magyarország Alaptörvényének VI. cikke értelmében mindenkinek joga van személyes adatai védelméhez, valamint a közérdekű adatok megismeréséhez és terjesztéséhez. A személyes adatok védelméhez és a közérdekű adatok megismeréséhez való jog érvényesülését sarkalatos törvénnyel létrehozott, független hatóság ellenőrzi. Ez a hatóság a Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: NAIH).

(2) Adatkezelő kiemelten fontosnak tartja a személyes adatok védelmét és azok bizalmas kezelését, valamint a vonatkozó, hatályos jogszabályoknak megfelelve, a közérdekű, ill. közérdekből nyilvános adatok minél szélesebb körű nyilvánosságra hozatalát. Az Adatkezelő ADATVÉDELMI SZABÁLYZATA (a továbbiakban: Szabályzat) az Adatkezelőnél vezetett nyilvántartásokra vonatkozó legfontosabb adatvédelmi szabályokat, elveket tartalmazza, különös tekintettel az adatkezeléssel, adatfeldolgozással, adattovábbítással, adatvédelemmel és az egyes adatok nyilvánosságra hozatallal kapcsolatos követelményekre. A Szabályzat célja, hogy a vonatkozó jogszabályok előírásai szerint, az érintettek érdekeinek megfelelően szabályozza az Adatkezelő működésével kapcsolatos

adatok kezelését és a feladatkörébe tartozó adatok feldolgozásának, továbbításának, hozzáférhetőségének feltételeit, módját.

(3) Jelen szabályzat célja, hogy meghatározza az Adatkezelőnél vezetett nyilvántartások törvényes rendjét, valamint biztosítsa az adatvédelem alkotmányos elveinek, az információs önrendelkezési jognak és az adatbiztonság követelményeinek érvényesülését, megakadályozza a jogosulatlan hozzáférést, az adatok jogosulatlan megváltoztatását és nyilvánosságra hozatalát.

(4) *Szabályzat személyi hatálya (1):* Jelen szabályzat személyi hatálya kiterjed az Adatkezelővel munkavállalói, megbízási vagy más munkavégzésre irányuló egyéb jogviszonyban állószemélyekre.

(5) *Szabályzat személyi hatálya (2):* Jelen szabályzat személyi hatálya kiterjed továbbá mindazon, magát digitálisan vagy fizikailag azonosító természetes személyekre is, akik az Adatkezelővel nem állnak a fenti bekezdés szerinti jogviszonyban, azonban

a) ezen jogviszony létesítése céljából adataikat az Adatkezelő kezeli,
b) adataikat jogszabályi előírás folytán az Adatkezelő a jogviszony megszűnését követően kezelni köteles.

(6) *Szabályzat tárgyi hatálya*: Jelen szabályzat tárgyi hatálya kiterjed az Adatkezelő által kezelt, jogszabály alapján személyes, közérdekű vagy közérdekből nyilvános adatra, különös tekintettel a bizalmi szolgáltatások által szerzett személyes adatokra.

A jelen szabályzat hatálya nem terjed ki az informatikai eszközökkel összefüggő technikai adatvédelemre, amelyről az ARCHIVÁLÁSI ÉS MENTÉSI SZABÁLYZAT rendelkezik.

(7) *Szabályzat területi hatálya*: Az EU 2016/679 számú Rendelete (továbbiakban: GDPR-Rendelet) értelmében jelen szabályzat hatálya kiterjed a személyes adatoknak az Unióban tevékenységi hellyel rendelkező adatkezelők vagy adatfeldolgozók tevékenységeivel összefüggésben végzett kezelésére, függetlenül attól, hogy az adatkezelés az Unió területén történik vagy nem.

(8) A vonatkozó GDPR-Rendelet szerint: „E rendeletet kell alkalmazni az Unióban tartózkodó érintettek személyes adatainak az Unióban tevékenységi hellyel nem rendelkező adatkezelő vagy adatfeldolgozó által végzett kezelésére, ha az adatkezelési tevékenységek:

a) áruknak vagy szolgáltatásoknak az Unióban tartózkodó érintettek számára történő nyújtásához kapcsolódnak, függetlenül attól, hogy az érintettnek fizetnie kell-e azokért; vagy

b) az érintettek viselkedésének megfigyeléséhez kapcsolódnak, feltéve hogy az Unió területén belül tanúsított viselkedésükről van szó.”

2. Fogalom-meghatározások

A Szabályzat alkalmazása során az EU GDPR-Rendeletében foglaltak szerint:

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

2. „adatkezelés”: a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés,

rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés, továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés;

3. „az adatkezelés korlátozása”: a tárolt személyes adatok megjelölése jövőbeli kezelésük korlátozása céljából;

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

5. „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;

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

7. „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;

8. „adatfeldolgozó”: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel;

9. „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 egyegyedi 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;

10. „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;

11. „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;

12. „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;

13. „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;

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

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

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

17. „tevékenységi központ”:

a) az egynél több tagállamban tevékenységi hellyel rendelkező adatkezelő esetében az Unión belüli központi ügyvitelének helye, ha azonban a személyes adatok kezelésének céljaira és eszközeire vonatkozó döntéseket az adatkezelő egy Unión belüli másik tevékenységi helyén hozzák, és az utóbbi tevékenységi hely rendelkezik hatáskörrel az említett döntések végrehajtatására, az említett döntéseket meghozó tevékenységi helyet kell tevékenységi központnak tekinteni;

b) az egynél több tagállamban tevékenységi hellyel rendelkező adatfeldolgozó esetében az Unión belüli központi ügyvitelének helye, vagy ha az adatfeldolgozó az Unióban nem rendelkezik központi ügyviteli hellyel, akkor az adatfeldolgozónak az az Unión belüli tevékenységi helye, ahol az adatfeldolgozó tevékenységi helyén folytatott tevékenységekkel összefüggésben végzett fő adatkezelési tevékenységek zajlanak, amennyiben az adatfeldolgozóra e rendelet szerint meghatározott kötelezettségek vonatkoznak;

18. „képviselő”: az, az Unióban tevékenységi hellyel, illetve lakóhellyel rendelkező és az adatkezelő vagy adatfeldolgozó által a 27. cikk alapján írásban megjelölt természetes vagy jogi személy, aki, illetve amely az adatkezelőt vagy adatfeldolgozót képviseli az adatkezelőre vagy adatfeldolgozóra az e rendelet értelmében háruló kötelezettségek vonatkozásában;

19. „vállalkozás”: gazdasági tevékenységet folytató természetes vagy jogi személy, függetlenül a jogi formájától, ideértve a rendszeres gazdasági tevékenységet folytató személyegyesítő társaságokat és egyesületeket is;

20. „vállalkozáscsoport”: az ellenőrző vállalkozás és az általa ellenőrzött vállalkozások;

21. „kötelező erejű vállalati szabályok”: a személyes adatok védelmére vonatkozó szabályzat, amelyet az Unió valamely tagállamának területén tevékenységi hellyel rendelkező adatkezelő

vagy adatfeldolgozó egy vagy több harmadik országban a személyes adatoknak az ugyanazon vállalkozáscsoporton vagy közös gazdasági tevékenységet folytató vállalkozások ugyanazon csoportján belüli adatkezelő vagy adatfeldolgozó részéről történő továbbítása vagy ilyen továbbítások sorozata tekintetében követ;

22. „felügyeleti hatóság”: egy tagállam által az 51. cikknek megfelelően létrehozott független közhatalmi szerv;

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

24. „személyes adatok határokon átnyúló adatkezelése”:

a) személyes adatoknak az Unióban megvalósuló olyan kezelése, amelyre az egynél több tagállamban tevékenységi hellyel rendelkező adatkezelő vagy adatfeldolgozó több tagállamban található tevékenységi helyein folytatott tevékenységekkel összefüggésben kerül sor; vagy

b) személyes adatoknak az Unióban megvalósuló olyan kezelése, amelyre az adatkezelő vagy az adatfeldolgozó egyetlen tevékenységi helyén folytatott tevékenységekkel összefüggésben kerül sor úgy, hogy egynél több tagállamban jelentős mértékben érint vagy valószínűsíthetően jelentős mértékben érint érintetteket;

25. „releváns és megalapozott kifogás”: a döntéstervezettel szemben benyújtott, azzal kapcsolatos kifogás, hogy ezt a rendeletet megsértették-e, illetve hogy az adatkezelőre vagy az adatfeldolgozóra vonatkozó tervezett intézkedés összhangban van-e a rendelettel; a kifogásban egyértelműen be kell mutatni a döntéstervezet által az érintettek alapvető jogaira és szabadságaira, valamint adott esetben a személyes adatok Unión belüli szabad áramlására jelentett kockázatok jelentőségét;

26. „az információs társadalommal összefüggő szolgáltatás”: az (EU) 2015/1535 európai parlamenti és tanácsi irányelv (1) 1. cikke (1) bekezdésének b) pontja értelmében vett szolgáltatás;

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

28. „Önkormányzati ASP rendszer”: a Magyarország helyi önkormányzatairól szóló 2011. évi CLXXXIX. törvény (a továbbiakban: Mötv.) 114. § (2) bekezdése szerinti, a helyi önkormányzatok, valamint gazdálkodási szakrendszer esetében az önkormányzat által alapított költségvetési szerv feladatellátását támogató, számítástechnikai hálózaton keresztül távoli alkalmazásszolgáltatást (Application Service Provider, ASP) nyújtó elektronikus információs rendszer.

Az EU GDPR-rendeletében meghatározottakon túl:

(1) „érintett”: bármely meghatározott, személyes adat alapján azonosított vagy - közvetlenül vagy közvetve - azonosítható természetes személy;

(2) „hozzájárulás”: az érintett akaratának önkéntes és határozott kinyilvánítása, amely

megfelelő tájékoztatáson alapul, és amellyel félreérthetetlen beleegyezését adja a rá vonatkozó személyes adat - teljes körű vagy egyes műveletekre kiterjedő - kezeléséhez;

(3) „tiltakozás”: az érintett nyilatkozata, amellyel személyes adatának kezelését kifogásolja, és az adatkezelés megszüntetését, illetve a kezelt adat törlését kéri;

(4) „adatvédelem”: a személyes és különleges adatok kezelésének normatív szabályozása az adatalany információs önrendelkezési jogának érvényesítése érdekében;

(5) „információs önrendelkezési jog”: az Alaptörvény VI. cikkében biztosított személyes adatok védelméhez való jognak az a tartalma, hogy mindenki maga rendelkezik személyes adatainak feltárásáról és felhasználásáról;

(6) „adattovábbítás”: az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele;

(7) „nyilvánosságra hozatal”: az adat bárki számára történő hozzáférhetővé tétele;

(8) „adattörlés”: az adat felismerhetetlenné tétele oly módon, hogy a helyreállítása többé nem lehetséges;

(9) „adatmegjelölés”: az adat azonosító jelzéssel ellátása annak megkülönböztetése céljából;

(10) „adatzárolás”: az adat azonosító jelzéssel ellátása további kezelésének végleges vagy meghatározott időre történő korlátozása céljából;

(11) „adatmegsemmisítés”: az adatot tartalmazó adathordozó teljes fizikai megsemmisítése;

(12) „adatfeldolgozás”: az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől, feltéve hogy a technikai feladatot az adaton végzik;

(13) „adatállomány”: az egy nyilvántartásban kezelt adatok összessége;

(14) „adatbiztonság”: a személyes adatok jogosulatlan kezelése, így különösen megszerzése, feldolgozása, megváltoztatása és megsemmisítése elleni szervezési, technikai megoldások és eljárási szabályok összessége; az adatkezelésnek az az állapota, amelyben a kockázati tényezőket - és ezzel a fenyegetettséget - a szervezési, műszaki megoldások és intézkedések a legkisebb mértékűre csökkentik;

(15) „adatgazda”: a Hatóság vezetője, vagy aki az adott adatkezelésre vonatkozó döntési jogosultsággal rendelkezik, illetve annak az adatkezelői egységnek a vezetője, ahová jogszabály vagy más közjogi szervezetszabályozó eszköz az adat kezelését rendeli, illetve ahol az adat keletkezik;

(16) „betekintési és megismerési jogosultság”: az a jogkör, amelynek birtokában a jogosult számára elérhetővé, megismerhetővé válnak az adott adatállományban kezelt személyes és különleges adatok;

(17) „közvetlen megismerési jogosultság”: adott adatállomány informatikai alkalmazás igénybevételével kezelt adatainak megismeréséhez adott olyan jogkör, amely a jogosult számára lehetőséget biztosít arra, hogy az ott kezelt adatokhoz az általa megválasztott időpontban közvetlen lekérdezéssel hozzáférjen;

(18) „közvetlen lekérdezés”: adott adatállományban kezelt adatokban - az adatkezelő által előzetesen rendelkezésre bocsátott általános lekérdezési jogosultság felhasználásával - előre meghatározatlan időpontban és alkalommal, naplózott formában történő betekintés, illetve az így megismerhetővé vált információ kinyomtatása vagy más módon történő rögzítése;

(19) „adathordozó”: bármely alakban, bármilyen eszköz felhasználásával és bármilyen eljárással előállított, személyes vagy különleges adatot tartalmazó anyag;

(20) „hardver eszköz”: valamennyi olyan eszköz, amelynek feladata az informatikai rendszer folyamatos működésének biztosítása, vagy amely biztonsági adatmentésre, avagy másolatok készítésére szolgál, valamint amely elektronikus vagy egyéb módon a számítógép külső behatás elleni védelmét szolgálja;

(21) 29. „bizalmi szolgáltatás”: az eIDAS Rendelet 3. cikk 16. pontja szerinti szolgáltatás;

(22) 30. „digitális állampolgárság”: az állampolgárok azon joga, amellyel digitálisan ügyet intézhetnek, szolgáltatást vehetnek igénybe;

(23) 31. „digitális állampolgár azonosító”: matematikai módszerrel képzett, különleges adatra nem utaló számjegysor, amely egyedi és tartós azonosítóként a polgárt a digitális térben egyértelműen azonosítja.

II. ÁLTALÁNOS ADATKEZELÉSI SZABÁLYOK

1. Az adatvédelem, adatbiztonság és adatkezelés szervezete

(1) Az adatkezelő adatkezelési szervezetének vezetője a jegyző. A jegyző ebben a minőségében:
   a. jóváhagyja a személyes és különleges adatokat tartalmazó, adatszolgáltatási, adattovábbítási, valamint az adatvédelemmel és adatkezeléssel kapcsolatos nyilvántartásokat;
   b. engedélyezi a nyilvántartási rendszerekhez a hozzáférési jogosultságot;
   c. szükség esetén gondoskodik az adatvédelmi ismeretek oktatásáról;
   d. a tudomására jutott visszásság esetén utasítja az érintett foglalkoztatottat a jogszerűtlen adatkezelés megszüntetésére, szükség esetén fegyelmi eljárást kezdeményez a foglalkoztatottal szemben és értesíti az incidensről az adatvédelmi tisztviselőt;
   e. folyamatosan tartja a kapcsolatot az adatvédelmi tisztviselővel.

(2) Az adatkezelői egységek vezetői:
   a. kötelesek gondoskodni a jelen szabályzatban foglaltak betartásáról és betartatásáról;
   b. kötelesek a jelen Szabályzatban foglaltakat megismerni, munkájuk során alkalmazni, valamint gondoskodni arról, hogy azt az egyes irodákon, osztályokon dolgozók megismerjék, előírásait munkavégzésük során betartsák, alkalmazzák;
   c. jogszabályváltozás vagy más fontos okból javaslatot tesznek a jegyzőnek jelen Szabályzat módosítására, kiegészítésére;
   d. a területeiken a hozzájuk érkező, adatkezeléssel kapcsolatos panaszokat kivizsgálják és a kivizsgálás eredményéről tájékoztatják a jegyzőt.

(3) Az informatikai eszközökkel összefüggő technikai adatvédelemért az informatikus a vonatkozó, az Adatkezelő GDPR-csomagjában foglalt szabályzatok által meghatározottak szerint felelős.

2. Az adatvédelmi tisztviselő

(1) Az Adatkezelő adatvédelmi tisztviselőjét a fenntartó vezető tisztviselői (polgármester és a jegyző) bízzák meg.

(2) A megbízott adatvédelmi tisztviselő adatait és elérhetőségeit az adatkezelő intézmény honlapján közzé kell tenni.

(3) Az adatvédelmi tisztviselő a következő nyilvántartásokat vezeti:
   a. a tudomására jutott **adatvédelmi incidenssel kapcsolatos intézkedések** ellenőrzése, valamint az incidenssel érintett személy(ek) tájékoztatása céljából **az Adatkezelő munkatársai által vezetett és az adatvédelmi tisztviselő részére a jelen szabályzat II.5. pontjában foglaltak szerint hozzáférhetővé tett adattáblák nyilvántartása,** amely egybefogja az egyes részlegek, osztályok tábláit és tartalmazza az érintett személyes adatok körét, az adatvédelmi incidenssel érintettek körét és számát, az adatvédelmi incidens időpontját, körülményeit, hatásait és az elhárítására megtett intézkedéseket, valamint az adatkezelést előíró jogszabályban meghatározott egyéb adatokat az ADATVÉDELMI INCIDENS-KEZELÉSI SZABÁLYZAT-ban meghatározottak szerint;
   b. az adattovábbítás jogszerűségének ellenőrzése, valamint az érintett tájékoztatása céljából

az Adatkezelő munkatársai és egyes részlegei által vezetett és az adatvédelmi tisztviselő részére a jelen szabályzat II.5. pontjában foglaltak szerint hozzáférhetővé tett adattáblák alapján **adatkezelési és adattovábbítási nyilvántartást** vezet, amely egybefogja az egyes részlegek, osztályok tábláit és tartalmazza az általa kezelt személyes adatok továbbításának időpontját, az adattovábbítás jogalapját és címzettjét, a továbbított személyes adatok körének meghatározását, valamint az adatkezelést előíró jogszabályban meghatározott egyéb adatokat a jelen Szabályzat IV. szakaszában és 3. számú mellékletében meghatározottak, majd elkészültét követően a hatályos INFORMÁCIÓ-ÁTADÁSI SZABÁLYZAT szerint. A nyilvántartás vezetésének elsődleges eszköze és helye az ADATVÉDELMI TÁRHÁZ, illetve az oda feltöltött és évente két alkalommal felülvizsgált nyilvántartási adattáblák.

c. Amennyiben szükségessé válik Adatvédelmi hatásvizsgálat elvégzése, úgy az adatvédelmi tisztviselő nyilvántartást vezet **az adott intézmény vezetőjének megbízásából lefolytatott Adatvédelmi hatásvizsgálatról,** annak eredményéről és a hatásvizsgálat kapcsán megtett intézkedésekről.

(4) A (2) bekezdésben meghatározottakon túlmenően az adatvédelmi tisztviselő legalább a következő feladatokat ellátja:

a. megkeresésre tájékoztat és szakmai tanácsot ad az Adatkezelő vagy az Adatfeldolgozó, továbbá az adatkezelést végző alkalmazottak részére az e rendelet, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezések szerinti kötelezettségeikkel kapcsolatban;

b. ellenőrzi az EU GDPR-Rendeletnek, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezéseknek, továbbá az Adatkezelő vagy az Adatfeldolgozó személyes adatok védelmével kapcsolatos belső szabályainak való megfelelést, ideértve a feladatkörök kijelölését, az adatkezelési műveletekben résztvevő személyzet tudatosság-növelését és képzését, valamint a kapcsolódó auditokat is;

c. kérésre, megkeresésre, a GDPR-Rendelet 35. cikk (2) bekezdése értelmében szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, valamint nyomon követi a minőségirányítás által vagy megbízásából lefolytatott hatásvizsgálat 35. cikk szerinti elvégzését;

d. együttműködik a felügyeleti hatósággal; és

e. az adatkezeléssel összefüggő ügyekben – ideértve a 36. cikkben említett előzetes konzultációt is – kapcsolattartó pontként szolgál a felügyeleti hatóság felé, valamint adott esetben bármely egyéb kérdésben konzultációt folytat vele.

(5) Az adatvédelmi tisztviselő a feladatait az adatkezelési műveletekhez fűződő kockázatok megfelelő figyelembevételével, az adatkezelés jellegére, hatókörére, körülményére és céljára is tekintettel végzi.

3. Az adatvédelem alapelvei (1)

(1) Jelen szabályzat az EU GDPR-Rendelet II. Fejezet, 5. cikkére alapozva a következő alapelvekre támaszkodik:

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

(2) Az Adatkezelő munkavállalói és külső megbízottjai (a továbbiakban: alkalmazottai) a feladataik ellátása körében személyes és különleges adatot csak a vonatkozó jogszabályok előírásainak betartásával kezelhetnek.

(3) A személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történjen, és azokat ne kezeljék ezekkel a célokkal össze nem egyeztethető módon. Az EU GDPR-Rendelet 89. cikk (1) bekezdésének megfelelően nem minősül az eredeti céllal össze nem egyeztethetőnek a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból történő további adatkezelés.

(4) A gyűjtött, tárolt és kezelt személyes adatok az adatkezelés céljai szempontjából megfelelőnek és relevánsnak kell, hogy legyenek, és a szükséges mértékre kell korlátozódniuk.

(5) A gyűjtött, tárolt és kezelt személyes adatoknak pontosnak és szükség esetén naprakésznek kell lenniük; minden ésszerű intézkedést meg kell tenni annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul töröljék vagy helyesbítsék.

(6) 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 ennél hosszabb ideig történő tárolására csak akkor kerülhet sor, amennyiben a személyes adatok kezelésére az EU GDPR-Rendelet 89. cikk (1) bekezdésének megfelelően közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból kerül sor.

(7) A személyes adatok kezelését oly módon kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve.

(8) Az Adatkezelő felelős az alapelvekben foglaltaknak való megfelelésért, továbbá képesnek kell lennie e megfelelés igazolására („elszámoltathatóság”).

(9) Személyes adat akkor kezelhető, amennyiben legalább az alábbiak 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.

(10) Személyes adat megfelelő jogalap fennállása esetén is csak megfelelő tájékoztatás kíséretében és megfelelő tájékoztatást követően kezelhető.

(11) Ha az adatkezelés hozzájáruláson alapul, az Adatkezelőnek képesnek kell lennie annak igazolására, hogy az érintett személyes adatainak kezeléséhez hozzájárult.

(12) Ha az érintett hozzájárulását olyan írásbeli nyilatkozat keretében adja meg, amely más ügyekre is vonatkozik, a hozzájárulás iránti kérelmet ezektől a más ügyektől egyértelműen megkülönböztethető módon kell előadni, érthető és könnyen hozzáférhető formában, világos és egyszerű nyelvezettel. Az érintett hozzájárulását tartalmazó ilyen nyilatkozat bármely olyan része, amely sérti e rendeletet, kötelező erővel nem bír.

(13) Az érintett jogosult arra, hogy hozzájárulását bármikor visszavonja. A hozzájárulás visszavonása nem érinti a hozzájáruláson alapuló, a visszavonás előtti adatkezelés jogszerűségét.

4. Az adatkezelés alapelvei (2)

(1) Adatkezelő a nem szándékosan közölt személyes adatokat nem őrzi meg és nem adja tovább.

(2) Az adatkezelés célhoz kötöttsége és arányossága: Adatkezelő személyes adatot csak meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében, a vonatkozó jogszabályoknak megfelelően kezel.

(3) Az adatok minőségére vonatkozó elv: Adatkezelő a személyes adatok felvételét és kezelését csak a vonatkozó jogszabályoknak megfelelően végzi. Ügyel az adatok pontosságára, teljességére és időszerűségére, valamint azok tárolására. Az adatokat oly módon kell tárolni, hogy az érintettet csak a tárolás céljához szükséges ideig lehessen azonosítani.

(4) Különleges adatok védelme: A vonatkozó EU GDPR-Rendeletnek megfelelően Adatkezelőnél különleges érzékeny adat akkor kezelhető, ha az adatkezelésnek van a GDPR 6. cikkben meghatározott jogalapja és az alábbi esetek valamelyike fennáll:

a) az adatkezeléshez az érintett írásban hozzájárul; vagy

b) az adat gyűjtése és használata nemzetközi egyezményen alapul, vagy Alaptörvényben biztosított alapvető jog érvényesítése, továbbá a nemzetbiztonság, a bűnmegelőzés vagy a bűnüldözés érdekében törvény elrendeli; vagy

c) egyéb esetekben azt a törvény elrendeli.

(5) Az önkormányzati működéssel kapcsolatos vagy üzleti titkot képező adatok védelme: az önkormányzati működéssel kapcsolatos vagy üzleti titok kiemelten védendő adat. Amit Adatkezelő vagy bármely minőségbeli partnere üzleti titoknak minősít, az kívülálló személynek nem adható meg, kivéve ha:

a) ha ahhoz a partner előzetesen, írásban hozzájárult;

b) hatóság, bíróság kéri;

c) az adat közérdekű vagy közérdekből nyilvános adatnak minősül;

d) jogszabály alapján egyéb okból kötelező kiadni.

(6) Adatbiztonság: Adatkezelő mindent megtesz az általa kezelt, illetőleg nála feldolgozás alatt lévő adatok biztonsága érdekében.

(7) Érintettek tájékoztatása: Az érintettekkel az adat felvétele előtt közölni kell, hogy az adatszolgáltatás önkéntes vagy kötelező. Kötelező adatszolgáltatás esetén meg kell jelölni az adatkezelést elrendelő jogszabályt is.

(8) Ha az adatkezelő által kezelt személyes adatok nem teszik lehetővé az adatkezelő számára valamely digitális állampolgárként eljáró természetes személy *azonosítását*, akkor az adatkezelőt nem lehet arra kötelezni, hogy – kizárólag az ezen szabályzat valamely rendelkezésének való megfelelés céljából – az érintett személyazonosságának megállapítása érdekében további információkat szerezzen be. Az adatkezelő ugyanakkor nem utasíthatja vissza az érintett által a jogai gyakorlásának támogatása érdekében nyújtott további információkat. Az *azonosítás* magában foglalja az érintettek például olyan hitelesítési mechanizmus révén történő digitális azonosítását, amelynek keretében az érintett ugyanazokat a belépési azonosító adatokat adja meg, amelyeket az adatkezelő által nyújtott online szolgáltatáshoz történő bejelentkezéshez használ.

5. Adatkezeléssel kapcsolatos kötelező nyilvántartások és bejelentési kötelezettség

(1) 2018. május 25. napjától az Európai Unió valamennyi tagállamában alkalmazandó általános adatvédelmi rendelet (EU GDPR-rendelet) értelmében két esetben merül fel bejelentési kötelezettség: az adatvédelmi tisztviselő nevét és elérhetőségét, továbbá az adatvédelmi incidenseket kell az illetékes hatóságnak bejelenteni.

(2) Az általános adatvédelmi rendelet (EU GDPR-Rendelet) 30. cikke szerint az adatkezelők, illetve adatfeldolgozók kötelezettsége, hogy az általuk végzett adatkezelési tevékenységekről vezessenek nyilvántartást. Az adatkezelőknek, adatfeldolgozóknak saját maguknak kell nyilvántartaniuk az adatkezeléseiket, azokat azonban nem kell bejelenteniük a Hatóság felé.

(3) ***Belső adatkezelési nyilvántartás*** → *VEZETI: INTÉZMÉNYVEZETŐK.*

→ *KAPJA HIVATALBÓL (adatvédelmi tárházba való feltöltés útján): ADATVÉDELMI TISZTVISELŐ*

A (9) pontban foglaltak szerinti adatkezelési tevékenységek nyilvántartása vezetendő az általános adatvédelmi rendeletben meghatározott adattartalommal a hivatalosan alkalmazott és rendszeresített Excel-táblában meghatározottak szerint.

(4) ***Adattovábbítási nyilvántartás*** → *VEZETI: INTÉZMÉNYVEZETŐK*

→ *KAPJA HIVATALBÓL (adatvédelmi tárházba való feltöltés útján): ADATVÉDELMI TISZTVISELŐ*

Az Adatkezelőnek az adattovábbítás jogszerűségének ellenőrzése, valamint az érintett tájékoztatása céljából adattovábbítási nyilvántartást kell vezetnie a a hivatalosan alkalmazott és rendszeresített Excel-táblában meghatározott adattartalommal a jelen Szabályzat IV. szakaszában meghatározottak szerint.

(5) A DPO által a jelen szabályzat II.2. (3) b) pontja értelmében gyűjtött adattovábbítási táblázatokból összeálló és az erre a célra létrehozott ADATVÉDELMI TÁRHÁZban tárolt központi adattovábbítási nyilvántartást személyes adat tekintetében öt évig, különleges (érzékeny) adat esetében 20 évig kell megőrizni.

(6) Nem kell nyilvántartást vezetni az Adatkezelőn belüli olyan személyes adatok továbbításáról, amely törvényi előíráson vagy felhatalmazáson alapul és a rendeltetésszerű munkavégzéshez szükséges.

(7) ***Nyilvántartás adatvédelmi incidensről*** → *VEZETI: ADATVÉDELMI TISZTVISELŐ AZ INTÉZMÉNYVEZETŐK ÁLTAL KITÖLTÖTT BEJELENTŐ LAPOK ALAPJÁN*

Az Adatkezelőnek az adatvédelmi incidenssel kapcsolatos intézkedések ellenőrzése, valamint az érintett tájékoztatása céljából nyilvántartást kell vezetnie A NAIH MINT FELÜGYELETI HATÓSÁG ÁLTAL RENDELKEZÉSRE BOCSÁTOTT NYOMTATVÁNYBAN meghatározott adattartalommal.

(8) ***Nyilvántartás elutasított közérdekű adatigénylési kérelmekről (amennyiben releváns)*** → *VEZETI: INTÉZMÉNY VEZETŐJE*

TÁJÉKOZTATÁST KAP ÉS MÁSOLATBAN GYŰJTI → ADATVÉDELMI TISZTVISELŐ

Az Adatkezelő az elutasított kérelmekről, valamint az elutasítások indokairól nyilvántartást köteles vezetni, és az abban foglaltakról minden évben január 31-éig tájékoztatni köteles a NAIH-ot A NAIH ÁLTAL ERRE A CÉLRA KIADOTT NYOMTATVÁNYON. A kitöltött és a NAIH számára benyújtott tájékoztató nyomtatványt lerakás és megőrzés céljából megkapja az Adatvédelmi tisztviselő is.

(9) A nyilvántartásokat az erre a célra hivatalosan rendszeresített **Excel-file szerint** vezető munkavállaló(k) a nyilvántartásokat kötelesek az erre a célra létrehozott **ADATVÉDELMI TÁRHÁZ-ba feltölteni.**

(10) A feltöltött összesítő táblákat a feltöltő intézmény vezetője évente KÉT ALKALOMMAL:

- **január első hetének utolsó munkanapján** és
- **az adott év július 1. napját követő első munkanapon**

köteles felülvizsgálni és **amennyiben változás állt be** a nyilvántartott adatok körét illetően vagy sor került adattovábbításra, úgy

1. **a változás(oka)t a már feltöltött táblába átvezeti és ott megjeleníti;**
2. **a változás(oka)t immáron magába foglaló új táblát a TÁRHÁZ-ba (ismét) feltölti;**
3. **elektronikus levélben tájékoztatja a DPO-t az eseményről.**

Változás vagy adattovábbítási esemény hiányában a féléves felülvizsgálat nem igényel további intézkedést vagy aktivitást.

(11) Az adatvédelmi célokra létrehozott TÁRHÁZ-hoz való hozzáférés rendje a következő:

- A rendszerhez korlátlanul (feltöltési, dokumentumkezelési és dokumentumszerkesztési jogosultsággal) hozzáférnek: adatvédelmi tisztviselő, jegyző, aljegyző
- A rendszerhez korlátozottan (dokumentumfeltöltési és dokumentum-megtekintési jogosultsággal) hozzáférnek: polgármester, a polgármesteri titkárság vezetője, a Polgármesteri Hivatal osztályvezetői, a Vecsési Városgondnok Nonprofit Kft. ügyvezető igazgatója, a Vecsési Városgondnok Nonprofit Kft. adatvédelemmel kapcsolatos ügyek intézésére kijelölt 1 fő munkavállalója, a Vecsés Város által fenntartott intézmények vezetői.

(12) Az ADATVÉDELMI TÁRHÁZ elérési útvonala a következő: portal.okosonkormanyzat.hu

(13) A rendszerhez az érintettek jelszóval férhetnek hozzá, amelyet jelszóval védett hozzáférést nem adhatják tovább. Ezen továbbadási tilalom a helyettesíts esetére is vonatkozik: betegség, szabadság vagy egyéb, helyettesítést igénylő helyzet esetén az ADATVÉDELMI TÁRHÁZ tekintetében nem a szokásos helyettesítési rend érvényesül. A helyettesítésre szoruló személy a TÁRHÁZ-zal kapcsolatos feladatait és ezzel az ahhoz való hozzáférését nem adhatja át másik személynek.

(14) Amennyiben adatvédelmi incidens esete forog fenn, az ADATVÉDELMI INCIDENS-KEZELÉSI SZABÁLYZAT rendelkezései lépnek életbe.

6. Az adatkezelés időtartama, az adatok törlése

(1) Az adatkezelés időtartama:

a) az adózás rendjéről szóló törvényben meghatározott személyes adatok,

b) a társadalombiztosítási ellátásokról szóló törvényben meghatározott személyes adatok,

c) a kötelező egészségbiztosítási törvényben meghatározott személyes adatok esetében a jogszabályban meghatározott megőrzési idő;

d) a menetlevelek kötelező használatát előíró jogszabályban meghatározott személyes adatok és

e) a közúti közlekedésben használt menetíró készülékek kötelező használatát előíró jogszabályban meghatározott személyes adatok

esetében az adatfelvételt követő 5. év utolsó napja, kivéve, ha jogszabály ennél hosszabb megőrzési időt ír elő;

f) egyéb esetekben: az adatkezelés az adatkezelés céljának megvalósulásáig történik, kivéve, ha jogszabály ettől eltérő megőrzési időt ír elő. Ezen adatok megőrzésére vonatkozó részletes szabályok Adatkezelő egyéb, az adatok kezeléséről rendelkező szabályaiban kerülnek kifejtésre.

(2) Az Adatkezelő az adatokat az adat rendelkezésére állásától kezdve az adatok törléséig kezeli.

(3) Az érintett jogosult arra, hogy kérésére az Adatkezelő indokolatlan késedelem nélkül törölje a rá vonatkozó személyes adatokat, az Adatkezelő pedig köteles arra, hogy az érintettre vonatkozó személyes adatokat indokolatlan késedelem nélkül törölje, ha az alábbi indokok valamelyike fennáll:

a) a személyes adatokra már nincs szükség abból a célból, amelyből azokat gyűjtötték vagy más módon kezelték;

b) az érintett visszavonja a 6. cikk (1) bekezdésének a) pontja vagy a 9. cikk (2) bekezdésének a) pontja értelmében az adatkezelés alapját képező hozzájárulását, és az adatkezelésnek nincs más jogalapja;

c) az érintett a 21. cikk (1) bekezdése alapján tiltakozik az adatkezelése ellen, és nincs elsőbbséget élvező jogszerű ok az adatkezelésre, vagy az érintett a 21. cikk (2) bekezdése alapján tiltakozik az adatkezelés ellen;

d) a személyes adatokat jogellenesen kezelték;

e) a személyes adatokat az Adatkezelőre alkalmazandó uniós vagy tagállami

jogban előírt jogi kötelezettség teljesítéséhez törölni kell;

f) a személyes adatok gyűjtésére az EU GDPR-Rendelet 8. cikk (1) bekezdésében említett, információs társadalommal összefüggő szolgáltatások kínálásával kapcsolatosan került sor;

g) azt bíróság vagy az adatvédelmi hatóság elrendelte.

(4) A személyes adatot tartalmazó iratot a jogszabályban vagy belső szabályzatban meghatározott idő elteltét követően irattárba kell helyezni és a hatályos IRATKEZELÉSI SZABÁLYZAT, illetve a törvényi szabályozás szerinti megőrzési időtartam lejáratával selejtezni kell vagy meg kell az adatot minden adathordozón semmisíteni.

7. Adatfeldolgozás

(1) Amennyiben az adatfeldolgozást maga az Adatkezelő nem tudja elvégezni, az adatfeldolgozással külső szervezet is megbízható. Az adatfeldolgozásra irányuló szerződésekre az általános szerződéskötési és közbeszerzési szabályok irányadóak. Az adatfeldolgozással nem bízható meg olyan szervezet, amely a feldolgozandó személyes adatokat felhasználó üzleti tevékenységben érdekelt.

(2) Az (1) bekezdés szerinti adatfeldolgozó kizárólag Adatkezelő hozzájárulásával és rendelkezéseinek, valamint a vonatkozó jogszabályoknak megfelelve vehet igénybe további adatfeldolgozót.

(3) Az igénybe vett adatfeldolgozók tevékenységüket csak az Adatkezelő Információ-biztonsági Rendszerének (IBR) szerint meghatározott előírások betartásával végezhetik.

III. SZEMÉLYES ADATOK VÉDELME

1. A személyes adatok védelme érdekében szükséges intézkedések

(1) Az Adatkezelő köteles az adatkezelési műveleteket úgy megtervezni és végrehajtani, hogy az biztosítsa az érintettek magánszférájának védelmét.

(2) Az Adatkezelővel jogviszonyban álló azon személyeknek (a továbbiakban: Adatkezelővel jogviszonyban állók), akik munkakörükből vagy beosztásukból kifolyólag személyes adat birtokába jutnak vagy ilyen adatot kezelnek, kötelességük ezen adatok védelme és bizalmas megőrzése.

(3) Az adatokat megfelelő, az IBR-ben meghatározott intézkedésekkel védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen.

(4) Amennyiben az Adatkezelővel jogviszonyban álló személy munkaköre vagy tisztsége alapján személyes, különleges, avagy bűnügyi személyes adatokba nyer betekintést, vagy azok birtokába jut, köteles az EU GDPR-Rendeletben és az Infotv.-ben foglaltaknak megfelelően eljárni, így különösen a személyes adatokat csupán az előre rögzített célra használhatja fel és az adatokat óvni kell az illetéktelen hozzáféréstől.

(5) Az Adatkezelővel jogviszonyban álló személyek felelősséggel tartoznak minden olyan kárért, amely a jelen szakaszban megfogalmazott adatkezelési, adatvédelmi kötelezettségük megszegéséből származik.

(6) Amennyiben Adatkezelő harmadik személlyel olyan, nem adatfeldolgozásra irányuló szerződéses jogviszonyt létesít, amelyben előírt feladat során személyes adatok kezelése valósul meg, a szerződésben kötelezően rögzíteni kell a vonatkozó jogszabályokban és a jelen szabályzatban foglaltak betartására vonatkozó kötelezettséget.

(7) Az Adatkezelő, valamint tevékenységi körében az általa megbízott adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat, az IBR-ben és a GDPR-csomagban foglalt technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek a vonatkozó jogszabályokban, valamint a jelen Szabályzatban foglaltaknak való megfelelést biztosítják.

(8) Az Adatkezelőnek és az általa megbízott adatfeldolgozónak az adatok biztonságát szolgáló intézkedések meghatározásakor és alkalmazásakor tekintettel kell lennie a technika mindenkori fejlettségére, valamint az adatbiztonságot érintő jogszabályi rendelkezésekre, és olyan döntést kell hoznia, amely leginkább garantálja az adatok biztonságát, kivéve, ha ez aránytalan nehézséggel vagy költséggel járna az Adatkezelő számára.

(9) A személyes adatok automatizált feldolgozása során az Adatkezelő és az Adatfeldolgozó további intézkedésekkel köteles biztosítani:

a) a jogosulatlan adatbevitel megakadályozását;

b) az automatikus adatfeldolgozó rendszerek jogosulatlan személyek általi, adatátviteli berendezés segítségével történő használatának megakadályozását;

c) annak ellenőrizhetőségét és megállapíthatóságát, hogy a személyes adatokat adatátviteli berendezés alkalmazásával mely szerveknek továbbítottak vagy továbbíthatják;

d) annak ellenőrizhetőségét és megállapíthatóságát, hogy mely személyes adatokat, mikor és ki vitte be az automatikus adatfeldolgozó rendszerekbe;

e) a telepített rendszerek üzemzavar esetén történő helyreállíthatóságát és

f) azt, hogy az automatizált feldolgozás során fellépő hibákról jelentés készüljön.

(10) Automatizált adatkezelés során felmerülő informatikai problémák naplózása, az erre való lehetőség megteremtése alapvetően az informatika rendszert fejlesztő szolgáltató feladata.

2. Tájékoztatási kötelezettség

(1) Minden adatkezelés előtt világossá kell tenni az érintettek számára, hogy adataik kezelése az érintett aktivitásával megvalósuló hozzájáruláson alapul vagy valamely jogszabályi előírás következtében kötelező, vagy egyéb, a GDPR Rendelet 6. cikke szerinti jogalap alapján történik. Az érintettet az adatkezelés megkezdése előtt – amennyiben azt valamely jogszabály kifejezetten nem tiltja – egyértelműen és részletesen tájékoztatni kell az adatai kezelésével kapcsolatos minden tényről, így különösen az adatkezelés céljáról és jogalapjáról, az adatkezelés időtartamáról, valamint arról, ha az érintett személyes adatait az Adatkezelő hozzájárulással, kötelezettségeinek teljesítése vagy harmadik személy jogos érdekeinek érvényesítése alapján kezelik, illetve arról, hogy kik ismerhetik meg az adatokat.

(2) A tájékoztatásnak ki kell terjednie az érintett adatkezeléssel kapcsolatos jogaira és jogorvoslati lehetőségeire is. Az (1) bekezdés szerinti tájékoztatást az Adatkezelővel *munkaviszonyt létesítő személyek részére* a jogviszony létrejöttekor, az általános, a Munka tv. szerint kötelező tájékoztatás keretében kell megadni.

(3) Adatkezelő *ügyfelei számára* az Adatkezelő az általa üzemeltetett honlapon elhelyezett **ADATVÉDELMI ÉS ADATKEZELÉSI TÁJÉKOZTATÓ-ban**, **valamint megkeresés, kérés, személyes ügyintézés esetén személyesen kell megadni.**

(4) A tájékoztatás nyújtására vonatkozó kötelezettség előírása nem szükséges, ha az érintettnek ez az információ már a birtokában van, vagy ha az adat megszerzését vagy közlését kifejezetten előírja az adatkezelőre alkalmazandó uniós vagy tagállami jog, amely az érintett jogos érdekeinek védelmét szolgáló megfelelő intézkedésekről rendelkezik, vagy ha az érintett tájékoztatása lehetetlennek bizonyul vagy aránytalanul nagy erőfeszítést igényelne. E helyzet állhat elő különösen akkor, ha az adatkezelés közérdekű archiválási célt, tudományos és történelmi kutatási célt vagy statisztikai célt szolgál. E tekintetben az érintettek számát, az adatok korát, valamint az elfogadott megfelelő garanciákat figyelembe kell venni.

3. Bizalmasság

(1) Az Adatkezelővel jogviszonyban állók kötelesek védeni és őrizni a munkakörükből, velük kötött szerződésből, tisztségükből adódó feladatok teljesítése során vagy azzal összefüggésben tudomásukra jutott adatokat, információkat, dokumentumokat, és kötelesek minden, tőlük joggal elvárható erőfeszítést megtenni annak érdekében, hogy azok megfelelő védelmét biztosítsák.

(2) Az (1) bekezdésben foglalt kötelezettségük teljesítése érdekében az Adatkezelővel jogviszonyban állóknak szellemi termék, kutatási eredmény, tananyag, találmány, stb. kezelését, tárolását elsősorban Adatkezelő eszközével, adatkezelői informatikai szolgáltatás esetében jóváhagyott szolgáltatási szerződés alapján kell biztosítaniuk. Ha ilyen jellegű anyagot Adatkezelőn kívül kezelnek, meg kell bizonyosodniuk arról, hogy a jelen és egyéb részletező szabályzatban foglaltak érvényesíthetők.

(3) Az Adatkezelővel jogviszonyban állók felelősséggel tartoznak minden olyan kárért, amely az (1)-(2) bekezdésben körülírt adatkezelési, titoktartási kötelezettségük megszegéséből származik.

4. A működés során keletkező adatok védelme

Adatkezelő munkatársai és szerződés keretében megbízott munkavállalói, szállítói kötelesek bizalmasan kezelni minden olyan adatot, információt vagy dokumentumot – függetlenül attól, hogy ahhoz milyen formában és milyen módon jutottak hozzá –, amely előttük a munkaköri feladataik teljesítése során vagy azzal összefüggésben vált vagy válik ismertté.

5. Az érintett jogai és azok érvényesítése

(1) Az adatvédelmi tisztviselő az Infotv. és a jelen Szabályzat rendelkezéseinek kivonatával tájékoztatást készít arról, hogy az érintettet milyen jogok illetik meg és azok megsértése esetén mi a jogorvoslat rendje, tájékoztatja az érintettet a NAIH-hoz és a bírósághoz fordulás jogáról és folyamatáról. A tájékoztatást Adatkezelő honlapján el kell helyezni.

(2) Az érintett az adatkezelést végző illetékes ügyintézőtől tájékoztatást kérhet a róla szóló adatkezelésről és jogosultsága igazolását követően abba bele is tekinthet. A betekintést úgy kell biztosítani, hogy ez alatt az érintett más személy adatait ne ismerhesse meg.

(3) Az érintett kérelmére az Adatkezelő tájékoztatást ad az általa kezelt adatairól, az adatkezelés céljáról, jogalapjáról, időtartamáról, az adatvédelmi incidens körülményeiről, hatásairól és az elhárítására megtett intézkedésekről, továbbá arról, hogy kik és milyen célból kapták meg az adatokat. Az Adatkezelő köteles a kérelem benyújtásától számított legfeljebb 8 munkanap alatt, közérthető formában, az érintett erre irányuló kérelmére írásban megadni a tájékoztatást.

(4) Adatváltozás vagy téves adatrögzítés észlelése esetén az érintett kérheti kezelt adatainak helyesbítését, illetve kijavítását, valamint személyes adatainak – a kötelező adatkezelés kivételével – törlését vagy zárolását. Az Adatkezelő köteles a kérelem benyújtásától számított legrövidebb idő, de legfeljebb 8 munkanap alatt az adatváltozást átvezetni, a téves adatot kijavítani és annak megtörténtéről a kérelmezőt tájékoztatni.

(5) Adatkezeléssel kapcsolatos jogainak megsértése esetén az érintett az adatvédelmi tisztviselőhöz fordulhat, aki a panaszt megvizsgálja, és ha az alapos, Adatkezelő vezetőjénél intézkedést kezdeményez, ellenkező esetben a panaszt elutasítja, erről a panaszost a kérelem kézhezvételét követő 30 napon belül írásban tájékoztatja a kérelem elutasításának ténybeli és jogi indokait is közölve. A kérelem elutasítása esetén a panaszost tájékoztatni kell a bírósági jogorvoslat, továbbá a Hatósághoz fordulás lehetőségéről.

(6) A kérelemre teljesített adattovábbításról, valamint az elutasított kérelmekről az érintett Adatkezelő jegyzőkönyvet köteles felvenni. A jegyzőkönyv vezetését a 2. sz. mellékletben meghatározottak szerint kell elvégezni. A jegyzőkönyv első példányát az adatkezelés helyén kell őrizni, második példányát pedig mellékleteivel együtt – másolat küldése esetén az „Eredetivel megegyező hiteles másolat” szövegezéssel és pecséttel ellátva – az adatvédelmi tisztviselőhöz kell továbbítani, aki köteles az elutasított kérelmekről a Hatóságot a tárgyévet követő év január 31-éig értesíteni. A jegyzőkönyvet öt évig kell megőrizni.

6. Az adatvédelmi incidenssel kapcsolatos rendelkezések

(1) Az Adatkezelő nyilvántartást vezet az adatkezelőnél vagy a megbízott adatfeldolgozójánál felmerülő adatvédelmi incidensekről. A nyilvántartás adattartalmát az ADATVÉDELMI INCIDENS-KEZELÉSI SZABÁLYZAT 2. SZ. MELLÉKLETÉBEN meghatározottak szerint kell vezetni.

(2) Az incidensekkel kapcsolatos rendelkezésekről és kommunikációról Adatkezelő ADATVÉDELMI INCIDENS-KEZELÉSI SZABÁLYZATA rendelkezik.

(3) Az ADATVÉDELMI INCIDENS-KEZELÉSI SZABÁLYZAT ÉRTELMÉBEN Adatkezelő munkavállalója vagy szerződéses partnere (adatfeldolgozó) a tudomására jutott incidens kapcsán mérlegeli, hogy az incidens érinti-e az adatvédelmet.

(4) Amennyiben az incidens adatvédelmet érint, Adatkezelő munkavállalója vagy szerződéses partnere (adatfeldolgozó) **az adatvédelmi incidens tényét haladéktalanul jelenti Adatkezelő adatvédelmi tisztviselőjének az adatvédelmi incidens-bejelentő nyomtatványon.**

(5) Adatkezelő munkavállalói részére előírás, hogy az adatvédelmi incidens-bejelentés és incidens-kezelés teljes folyamatát írásban dokumentálják a későbbi azonosíthatóság és bizonyíthatóság érdekében.

(6) A dokumentálás bizonyítékai (dokumentumok) az adatvédelmi tisztviselő jóváhagyását követően lerakásra (feltöltésre) kerülnek az **ADATVÉDELMI TÁRHÁZBA**.

(7) Adatkezelő képviselője az adatvédelmi tisztviselővel együttműködésben megvizsgálja, hogy sérültek-e az érintettek személyes jogai, az adatok titkosítottak voltak-e, az adatok védettek voltak-e (anonimizálás, álnevesítés), magas kockázattal járnak-e a személyes jogok sérülékenysége terén. Amennyiben a fenti feltételek vizsgálata pozitív (azaz nemkívánatos) eredményt ad, úgy az adatvédelmi incidenst az Adatkezelő az adatvédelmi tisztviselőn keresztül az illetékes felügyeleti hatóságnál jelenteni köteles.

(8) Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az Adatkezelőnek indokolatlan késedelem nélkül tájékoztatnia kell az érintettet az adatvédelmi incidensről. E tájékoztatásban világosan és közérthetően ismertetni kell az adatvédelmi incidens jellegét, és közölni kell legalább a következőket:

a) az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;

b) az adatvédelmi incidensből eredő, valószínűsíthető következményeket;

c) az Adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

(9) Az érintettet nem kell tájékoztatni, ha a következő feltételek bármelyike teljesül:

a) az Adatkezelő megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre, és ezeket az intézkedéseket az adatvédelmi incidens által érintett adatok tekintetében alkalmazták, különösen azokat az intézkedéseket - mint például a titkosítás alkalmazása -, amelyek a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik az adatokat;

b) az Adatkezelő az adatvédelmi incidenst követően olyan további intézkedéseket tett, amelyek biztosítják, hogy az érintett jogaira és

szabadságaira jelentett, magas kockázat a továbbiakban valószínűsíthetően nem valósul meg;

c) az egyedi tájékoztatás aránytalan erőfeszítést tenne szükségessé. Ilyen esetekben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, vagy olyan hasonló intézkedést kell hozni, amely biztosítja az érintettek hasonlóan hatékony tájékoztatását.

7. Adatvédelmi hatásvizsgálat

(1) Adatkezelő az adatvédelmi hatásvizsgálattal kapcsolatban a GDPR-rendelet vonatkozó részeit, különösképpen annak 35. cikkét tekinti kötelező érvénnyel betartandónak.

(2) Ha az adatkezelés valamely – különösen új technológiákat alkalmazó – típusa, figyelemmel annak jellegére, hatókörére, körülményére és céljaira, valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, akkor az Adatkezelő az adatkezelést megelőzően hatásvizsgálatot végez arra vonatkozóan, hogy a tervezett adatkezelési műveletek a személyes adatok védelmét hogyan érintik. Olyan egymáshoz hasonló típusú adatkezelési műveletek, amelyek egymáshoz hasonló magas kockázatokat jelentenek, egyetlen hatásvizsgálat keretei között is értékelhetőek.

(3) Adatkezelő az adatvédelmi hatásvizsgálat elvégzésekor az adatvédelmi tisztviselő szakmai tanácsát köteles kikérni.

(4) Ha az adatvédelmi hatásvizsgálat megállapítja, hogy az adatkezelés az Adatkezelő által a kockázat mérséklése céljából tett intézkedések hiányában valószínűsíthetően magas kockázattal jár, a személyes adatok kezelését megelőzően az Adatkezelő konzultál a felügyeleti hatósággal.

IV. ADATOK KEZELÉSE AZ ÖNKORMÁNYZAT ÁLTAL FENNTARTOTT INTÉZMÉNYEKNÉL

1. Az adatgyűjtés célja és az adatvédelmi nyilvántartás

Az adatkezelés célja annak biztosítása, hogy az Önkormányzat által fenntartott intézmények a feladataik ellátásához kapcsolódó ügyintézés során megfeleljenek az EU GDPR-Rendeletében és az Infotv.-ben meghatározott előírásoknak, valamint hatékonyan legyen képes kialakítani, fenntartani és szabályozni ügyfélkapcsolataikat.

2. A személyes adatok megszerzése és feldolgozása

2.1. Az Adatkezelő a személyes adatok megszerzésének időpontjában az érintett rendelkezésére kell, hogy bocsássa a következő információkat:

a. az Adatkezelőnek és – ha van ilyen – az Adatkezelő képviselőjének a kiléte és elérhetőségei;
b. az adatvédelmi tisztviselő elérhetőségei, ha van ilyen;
c. a személyes adatok tervezett kezelésének célja, valamint az adatkezelés jogalapja;
d. a 6. cikk (1) bekezdésének f) pontján alapuló („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.”) adatkezelés esetén, az Adatkezelő vagy harmadik fél már említett jogos érdekeit;
e. adott esetben a személyes adatok címzettjeit, illetve a címzettek kategóriáit, ha van ilyen;
f. adott esetben annak tényét, hogy az Adatkezelő harmadik országba vagy nemzetközi szervezet részére kívánja továbbítani a személyes adatokat.

2.2 Adatkezelő a 2.1. pontban megadott tájékoztatás mellett minden esetben meg kell, hogy adja a következő kiegészítő információkat:

a. a személyes adatok tárolásának időtartamáról, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjairól;
b. az érintett azon jogáról, hogy kérelmezheti az Adatkezelőtől a rá vonatkozó személyes adatokhoz való hozzáférést, azok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen, valamint az érintett adathordozhatósághoz való jogáról;
c. az adatkezeléshez való hozzájárulás bármely időpontban történő visszavonásához való jog, amely nem érinti a visszavonás előtt a hozzájárulás alapján végrehajtott adatkezelés jogszerűségét;
d. a felügyeleti hatósághoz címzett panasz benyújtásának jogáról;
e. arról, hogy a személyes adat szolgáltatása jogszabályon vagy szerződéses kötelezettségen alapul vagy szerződés kötésének előfeltétele-e, valamint, hogy az érintett köteles-e a személyes adatokat megadni, továbbá, hogy milyen lehetséges következményeikkel járhat az adatszolgáltatás elmaradása;
f. automatizált döntéshozatal ténye, ideértve a profilalkotást is, valamint legalább ezekben az

esetekben az alkalmazott logikára és arra vonatkozóan érthető információk, hogy az ilyen adatkezelés milyen jelentőséggel, és az érintettre nézve milyen várható következményekkel bír.

2.3. A fenti, 2.1-2.2. szerinti információkat abban az esetben és annyiban nem szükséges megadni, amilyen mértékben az érintett már rendelkezik az információkkal.

2.4. A 2.1-2.2. szerinti tájékoztatást

a. személyes ügyfélkezelés esetén szóban;

b. papír alapú nyomtatvány kitöltése esetén a nyomtatványon elhelyezett, legalább a részletes tájékoztatást (ADATVÉDELMI ÉS ADATKEZELÉSI TÁJÉKOZTATÓ) tartalmazó honlapra történő utalással, a jelen szabályzat **1. sz. mellékletében** foglalt szöveggel;

*c. amennyiben releváns: elektronikus ügyintézés esetén pedig az elektronikus nyomtatványon az érintett személyes adatainak kezelésére vonatkozó tájékoztatás elektronikus elérhetőségének a jelen szabályzat **1. sz. mellékletében** foglalt szöveggel történő elhelyezésével kell és lehetséges megadni.*

2.5. Az ügyfél a tájékoztatás 2.4.-ben leírt módon történő biztosítását követően papír alapú nyomtatvány esetében a nyomtatvány aláírásával, elektronikus nyomtatvány esetében annak továbbításával egyértelműen adja meg a tájékoztatáson alapuló hozzájárulását a nyomtatványon rögzített személyes adatainak kezeléséhez.

2.6. Az adatot fogadó munkavállaló a hozzájáruló nyilatkozatot tartalmazó nyomtatvány eredeti példányát az IRATKEZELÉSI SZABÁLYZAT-ban meghatározott előírások szerint köteles kezelni.

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

2.8. Adatkezelőnek biztosítania kell, hogy az érintett az Adatkezelőnél kezelt személyes adatait helyesbítse, javítsa.

3. Alkalmazotti nyilvántartásra vonatkozó különleges szabályok

(1) Jelen Szabályzat keretében munkaviszonnyal összefüggésben megvalósuló adatkezelésnek azon adatok kezelését nevezzük, melyek rögzítésének, nyilvántartásának és kezelésének jogszabályi alapját a Munka törvénykönyvéről szóló 2012. évi I. törvény, illetve annak végrehajtási rendeletei képezik.

(2) Az (1) pont értelmében az alkalmazotti nyilvántartás adatai a foglalkoztatottak munkaviszonyával kapcsolatos tények megállapítására, a besorolási követelmények igazolására és statisztikai adatszolgáltatásra, valamint a munkaviszonyokkal kapcsolatos szerződésekkel kapcsolatos ügyintézésre használhatók fel.

(3) Az alkalmazotti nyilvántartás Adatkezelő valamennyi, a (2) bekezdésben meghatározott alkalmazott adatát tartalmazza.

(4) Az alkalmazotti nyilvántartás adatait az érintett szolgáltatja.

(5) A bér- és munkaügyi nyilvántartásra az alkalmazotti nyilvántartásra vonatkozó rendelkezések irányadók.

(6) A bér- és munkaügyi nyilvántartás adatai a foglalkoztatott jogviszonyával kapcsolatos tények megállapítására, a besorolási követelmények igazolására, bérszámfejtésre, társadalombiztosítási ügyintézésre és statisztikai adatszolgáltatásra használhatók fel.

4. Az Adatkezelő által gyűjtött adatok köre és a gyűjtés célja

Adatkezelő az adatkezelés céljától függően az érintettek alábbi személyes adatait kezeli:

1. személyes ügyintézés során azonosított ügyfelek adatai,
2. különleges (érzékeny) adatok,
3. *amennyiben releváns: elektronikus ügyintézés során eredményes kérelmet benyújtott ügyfelek adatai.*

5. Adattovábbítás

5.1. Az Adatkezelőn belüli adattovábbítás

(1) Adatkezelőn belül a személyes adatok – a feladat elvégzéséhez szükséges mértékben és ideig – csak olyan Adatkezelői egységhez, személyhez továbbíthatók, amelynek, illetve akinek jogszabályban vagy az Adatkezelő Szervezeti és Működési Szabályzatában meghatározott tevékenysége ellátásához a személyes adatok megismerése és kezelése szükséges.

(2) Az Adatkezelőnél folyó, különböző célokra irányuló adatkezelések csak törvényes céloknak megfelelően, indokolt esetben kapcsolhatók össze.

5.2. Adattovábbítás megkeresés alapján, Adatkezelőn kívüli adattovábbítás

(1) Olyan megkeresés, amely az Adatkezelő által kezelt valamely személyes adat továbbítására irányul, csak jogszabályi előírás alapján vagy csak a (2) bekezdésben foglalt feltételek fennállása esetén teljesíthető. Minden más esetben az adattovábbítás teljesítését meg kell tagadni.

(2) Olyan esetben, amikor az adattovábbítás nem jogszabályi kötelezettségen alapul, az csak akkor teljesíthető, ha az érintett erre egyértelműen, aktív magatartást követően beleegyezik és aktivitásával Adatkezelőt felhatalmazza adatai továbbítására.

(3) Az érintett előzetesen is adhat ilyen tartalmú felhatalmazást, amely szólhat valamely időtartamra és/vagy a megkereséssel élő szervek meghatározott körére is.

(4) Azok az adatok, amelyek – a vonatkozó jogszabályok értelmében – nyilvánosak, vagy egyéb okból nyilvánosságra kerültek, megkeresésre közölhetők, vagy közölhető elérésük pontos helye, módja, elektronikus útvonala.

(5) Önkéntes adatszolgáltatás végrehajtását kizárólag az intézmény vezetője rendelhet el.

(6) Adatkezelő köteles biztosítani, hogy a munkavállaló a róla kezelt adatok továbbításáról tájékoztatást kapjon, a kezelt adatokat tartalmazó iratokról – külön kérésére vagy a Munka

tv. értelmében kötelező, a munkavállalói szerződés mellékletét képező tájékoztató keretében – másolatot vagy kivonatot kapjon.

5.3. A külföldre irányuló adattovábbítás

(1) Külföldre irányuló adattovábbítás esetén az adattovábbítást végzőnek külön meg kell győződnie arról, hogy a külföldre történő adattovábbítás EU GDPR-Rendeletben és a magyar Infotv.-ben meghatározott feltételei fennállnak-e.

(2) Ha az adattovábbítás az Európai Gazdasági Térség valamely államába irányul, úgy a személyes adatok megfelelő szintű védelmét nem kell vizsgálni.

5.4. A statisztikai célú adattovábbítás

(1) Az EU GDPR-Rendelete nem vonatkozik a statisztikai vagy kutatási célú adatkezelés céljából kezelt **anonim információkra.** Ebből fakadóan a statisztikai célú adatkezelés esetében a jelen Szabályzat III.2. fejezetében foglalt tájékoztatást sem kell megadni, ugyanakkor az EU GDPR-Rendelet előírásaira, különösképpen a Preambulum (62) és (156) szakaszában foglaltakra figyelemmel kell eljárni.

(2) A közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból folytatott adatkezelést összeegyeztethető, jogszerű adatkezelési műveleteknek kell tekinteni.

(3) Adatkezelő vállalja, hogy a személyes adatokat statisztikai célra kizárólag úgy adja át, hogy gondoskodik az adatok anonimitásáról vagy másképpen arról, hogy a továbbított adat(ok) az érintettel ne legyen(ek) kapcsolatba hozható(ak).

6. Egymáshoz kapcsolódó adatkezelések

Az érintett adatok másolása, azokból származtatott, az érintett azonosítására alkalmas új adatok létrehozása, más adatbázisokkal összekapcsolása új adatkezelésnek minősül, melyhez az Adatkezelőnek be kell szereznie az érintett hozzájárulását vagy rendelkeznie kell a megfelelő jogszabályi felhatalmazással.

Az adatokból képzett, a személy azonosítására alkalmas adatoktól megfosztott újonnan képzett adatokat az Adatkezelő statisztikák, belső kimutatások készítésére felhasználhatja.

7. Biztonsági követelmények

7.1. Számítógépen tárolt adatok

(1) Adatkezelő az informatikai rendszereket tűzfallal védi, és vírusvédelemmel látja el.

(2) A számítógépes levelező rendszert a munkavállalók csak munkakörükből fakadó munkavégzési célokra használhatják.

(3) Adatkezelő alkalmazottai a munkahelyi gépekhez **<u>külön engedély nélkül nem csatlakoztathatják</u>** saját számítástechnikai eszközeiket, adattároló és rögzítő

eszközeiket.

(4) Adatkezelő munkatársai számára az általuk kezelt személyes adatok interneten történő megosztása szigorúan tilos!

(5) A munkahelyen és az Adatkezelő eszközein file-letöltő-, torrent-, játék-, csevegő-, szexuális szolgáltatásokat kínáló oldalak látogatása szigorúan tilos, kivéve a szakalkalmazásokba beépített alkalmazásokat!

(6) A munkahelyi informatikai eszközökre külső programok letöltése csak a rendszergazda és a területi vezető jóváhagyását követően engedélyezett.

7.2. Manuális kezelésű adatok

A manuális kezelésű személyes adatok biztonsága érdekében az alábbi intézkedéseket kell foganatosítani:

a) az iktatott, és aktív használatban nem lévő iratokat jól zárható, száraz, tűzvédelmi és vagyonvédelmi berendezéssel ellátott helyiségben kell elhelyezni;

b) a folyamatos aktív kezelésben lévő iratokhoz csak az illetékes munkavállalók férhetnek hozzá, a személyzeti, a bér- és munkaviszonnyal kapcsolatos iratokat biztonságosan elzárva kell tartani;

A szabályzat 2025. január 01. napján lép hatályba.

Vecsés, 2025. január 1.”

……..

intézményvezető

1. **sz. melléklet: Adatvédelmi tájékoztató szöveg a Vecsés Város Önkormányzata által fenntartott intézmények által használt nyomtatványokra**

A személyes adatok kezelésével, azok kezelésének céljával és az adatkezelés biztonságával, valamint az ügyfelek jogaival kapcsolatos adatvédelmi tájékoztatás elérhető az intézmény honlapján, a www.vecsesigondozasikozpont.hu címen vagy igényelhető személyesen az intézmény munkatársainál.

Megismerési nyilatkozat

A leltározási és leltárkészítési szabályzatban foglaltakat megismertem. Tudomásul veszem, hogy az abban foglaltakat a munkavégzésem során köteles vagyok betartani.

Név	**Beosztás**	**Kelt**	**Aláírás**
Alácsné Gergely Krisztina	Intézményvezető helyettes	2025.01.01.	
Wieland Andrea	Gondozó	2025.01.01.	
Matasdi Fanni	Adminisztrátor	2025.01.01.	
Kristóf Ildikó	Gondozó	2025.01.01.	
Benéné Bíró Krisztina	Konyhai kisegítő	2025.01.01.	
Kátai-Szegedi Tímea	Konyhai kisegítő	2025.01.01.	
Lauter Józsefné	Gondozó	2025.01.01.	
Dobrovitzné F. Ágnes	Gondozó	2025.01.01.	
Dávidné Karacs Erika	Gondozó	2025.01.01.	
Stadinger Tímea	Gondozó	2025.01.01.	
Deim Andrásné	Gondozó	2025.01.01.	
Skupien Szilvia	Gondozó	2025.01.01.	
Ferencz Ildikó	Gondozó	2025.01.01.	
Stiller Nándorné	Takarító	2025.01.01.	
Oláh Nikoletta	Gondozó	2025.01.01.	
Kassai Krisztina	Gondozó	2025.01.01.	
Stiller Róza	Adminisztrátor	2025.01.01.	