A PÉCELI POLGÁRMESTERI HIVATAL

ADATVÉDELMI ÉS ADATBIZTONSÁGI

SZABÁLYZATA

Hatályos: 2018. 05. 18. napjától

Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban : Infotörvény) 24. § (1), (3) bekezdéseiben, a 30. § (6) bekezdésében és a 35. § (3) bekezdésében kapott felhatalmazás alapján a Péceli Polgármesteri Hivatalban (a továbbiakban: Hivatal) a polgárok személyi adatainak és lakcímének kezelésével kapcsolatos adatvédelmi szabályokat, a címnyilvántartásból [a továbbiakban: TSZR mint (Települési Szolgáltató Rendszer)] és a helyi szinten kezelt nyilvántartásból (a továbbiakban: vizuál regiszter) történő adatszolgáltatást és az adatbiztonság rendjét (a továbbiakban: Szabályzat) a következők szerint határozom meg:

A Szabályzat az alábbi jogszabályokon alapul:

- az Infotörvény;
- a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. törvény 17. § (2) bekezdés b) pontja és 21. §,
- a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. törvény végrehajtásáról rendelkező 146/1993. (X. 26.) Korm. rendelet 6–7 §, 8. § (1) bek. és 27. § (1) bek.,
- a minősített adat védelméről szóló 2009. évi CLV. törvény,
- az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény,
- az önkormányzati ASP rendszerről szóló 257/2016 (VIII.31.) Korm. rendelet,
- az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet.

1. A Szabályzat célja

A Szabályzat biztosítja a természetes személy (a továbbiakban: polgár) személyes adataival való önrendelkezési jogának, valamint az egyéb alkotmányos jogok érvényesítéséhez és a közigazgatás hatékonyságának biztosításához szükséges személyazonosító és lakcímadatok használatához fűződő közérdek összhangját.

A Szabályzat további célja, hogy biztosítsa a Hivatalban az alábbiakat:

- meghatározza a polgárok személyi és lakcím adatai kezelésének adatvédelmi szabályait,
- a papír alapú nyilvántartások esetén is megfelelően gondoskodjon a kezelő a fizikai megsemmisülés elleni védelméről, és arról, hogy e nyilvántartásokhoz csak a feladatok ellátására felhatalmazott személyek a feladatuk ellátásához szükséges mértékben férhessenek hozzá,
- a titok-, vagyon- és tűzvédelemre vonatkozó védelmi intézkedések betartását,
- az üzemeltetett számítógépek, informatikai eszközök, valamint azok kiegészítő eszközeinek rendeltetésszerű használatát,
- az üzembiztonságot szolgáló karbantartást és fenntartást,
- az adatok számítógépes feldolgozása és azok további hasznosítása során az illetéktelen felhasználásból származó hátrányos következmények megszüntetését, illetve minimális mértékre csökkentését,
- az adatállományok tartalmi és formai épségének megőrzését,
- adatállományok biztonságos mentését,
- a számítógépes rendszerek zavartalan üzemeltetését,
- a feldolgozás folyamatát fenyegető veszélyek megelőzését, elhárítását,
- az adatvédelem és adatbiztonság feltételeit,
- a védelem működését a rendszerek fennállásának egész időtartama alatt a megtervezésüktől kezdve az üzemeltetésükön keresztül a felhasználásig.

Jelen szabályzatban nem szereplő informatikai jellegű adatbiztonsági szabályokat a jelenleg hatályos Informatikai Biztonsági Szabályzat tartalmazza.

2. Értelmező rendelkezések

Az értelmező rendelkezések vonatkozásában az Infotörvény 3. §-ában írtak az irányadók.

3. A Szabályzat hatálya

3. 1. A szabályzat személyi hatálya a Hivatal valamennyi köztisztviselőjére, a Hivatalban foglalkoztatott munkavállalókra, közfoglalkoztatottra, illetve a számítástechnikai vagy egyéb üzemeltetési eljárásban részt vevő más szervezetek dolgozóira egyaránt kiterjed.

3. 2. Tárgyi hatálya kiterjed:

- a Hivatal teljes körű feladat- és hatáskörének ellátására,
- a védelmet élvező adatok teljes körére, felmerülésük és feldolgozási helyüktől, idejüktől és az adatok fizikai megjelenési formájától függetlenül,
- az adatok felhasználására, tárolására, továbbítására vonatkozó utasításokra,
- a Hivatal tulajdonában lévő valamennyi papír alapú, számítástechnikai, informatikai berendezésre, valamint ezek műszaki dokumentációra is,
- a számítástechnikai folyamatban szereplő összes dokumentációra (fejlesztési, szervezési, programozási, üzemeltetési dokumentáció),
- a rendszer- és felhasználói programokra, illetve a központilag tárolt adatokra.

4. Kapcsolódó szabályozások

4. 1. A szabályzatot a Hivatal Szervezeti és Működési Szabályzatával és egyéb szabályzatokkal összhangban kell alkalmazni.

4. 2. A közérdekű és a közérdekből nyilvános adatokról, a közzététel szabályairól a Hivatal közérdekű adatok megismerésére irányuló igények teljesítésének rendjére vonatkozó szabályzata rendelkezik.

5. Védelmet igénylő adatok, eszközök köre

5.1. A védelem tárgya:

- a Hivatal valamennyi szervezeti egységénél vezetett egyedi, illetve jogszabályban előírt nyilvántartás adattartalma;
- a Hivatal valamennyi szervezeti egységénél önkormányzati vagy hatósági eljárás során keletkezett személyes adat védelme;
- a törvényben meghatározott feltételek fennállása esetén adatszolgáltatás teljesítése a nyilvántartásból;
- közokiratok kiadása a nyilvántartott adatokról;
- a címnyilvántartásba felvett adatok, illetve a vizuál regiszterben található adatok kezelése,
- a Hivatal által használt ASP rendszer szakrendszereiben tárolt adatok.

5.2. A védelem eszközei
A mindenkori technikai fejlettségnek megfelelő műszaki, szervezeti, programozási, jogi, ügyrendi intézkedések azok az eszközök, amelyek a védelem tárgyának különböző veszélyforrásokból származó kárt okozó hatásokkal, szándékokkal szembeni megóvását elősegítik, illetve biztosítják.

6. Címnyilvántartás és adatszolgáltatás

6.1. A Hivatal megállapítja és a polgárok személyi adatainak, lakcímének nyilvántartását kezelő központi szervnek (a továbbiakban: központi szerv) továbbítja a települési címek nyilvántartását.

6.2. A címnyilvántartás tartalmazza
a) a település megnevezését,
b) a településrész nevét
c) a postai irányítószámot;
d) a közterület nevét és jellegét;
e) a ház számát, ezen belül az épület, lépcsőház, szint, emelet és ajtó számát, illetve megjelölését;
f) az ingatlan helyrajzi számát;
g) az ingatlan jellegét, technikai azonosítóját;
h) a tulajdonos vagy haszonélvező szállásadó nyilatkozatát a lakcímbejelentéshez történő hozzájárulásának módjáról;
i) a tulajdonos vagy haszonélvező szállásadó nyilatkozattételének időpontját;
j) a nyilatkozatot tevő tulajdonos vagy haszonélvező szállásadó személyi azonosítóját, ennek hiányában négy természetes személyazonosító adatát, továbbá értesítési címét;
k) a nyilatkozatot tevő nem természetes személy tulajdonos szállásadó nevét, székhelyét;
l) közös vagy osztatlan közös tulajdonú ingatlan esetén e tény feltüntetését;
m) a nyilatkozat visszavonásának időpontját, a hivatalbóli törlés időpontját és okát;
n) a szállásadó nyilatkozatát arról, hogy a lakcímbejelentésről a lakcím bejegyzésével egyidejűleg értesítést kér.

6.3. A címnyilvántartás 6.2. *a)–f)* pontjában meghatározott adatairól harmadik személy részére a központi szerv teljesít adatszolgáltatást az igényelt adatok körét megjelölő kérelmező részére.

6.4. A hivatali dolgozók az 1/a. számú melléklet szerinti nyomtatványon az aljegyző engedélyével kérhetnek adatszolgáltatást a vizuál regiszterből, illetve az 1/b. számú melléklet szerinti nyomtatványon a TSZR-ből, amelynek során az igényelt adatok körét és a kérelem jogcímét meg kell jelölni.

6.5. A Hivatal a 2. számú melléklet szerinti adattartalommal adattovábbítási nyilvántartást vezet.
Az adattovábbítási nyilvántartást, amennyiben személyes adatot tartalmaz 5 évig, ha különleges adatot tartalmaz, húsz évig kell megőrizni.

7. Nyilvántartások

7.1. A Hivatal a következő nyilvántartásokat vezeti:
a) adattovábbítási nyilvántartást, az általa teljesített adatszolgáltatásokról (lásd: 6.4. pont);
b) üzemeltetési naplót
c) adatvédelmi incidensek nyilvántartását (lásd: 8. pont)

7.2. A jegyző a 4. számú melléklet szerinti nyilvántartást vezeti azokról a köztisztviselőkről, akik az eljárás során jogosultak az egyes okmány-nyilvántartások adataihoz hozzáférni.
A nyilvántartás adatait a hozzáférési jogosultság megszűnésétől számított 5 évig kell megőrizni.

7.3. A közérdekű adatok megismerésére irányuló igények teljesítése esetén a betekintési igényeket a Hivatal elkülönítetten, a közérdekű adatok megismerésére irányuló igények teljesítésének rendjéről szóló szabályzatban foglaltak szerint tartja nyilván.

7.4. A Hivatal a nyilvántartás rendszerének felépítése, a jogosultságok meghatározása és egyéb szervezeti intézkedések útján gondoskodik arról, hogy a személyes adatokat tartalmazó adathordozókat csak azon személyek ismerhessék meg, akiknek erre a feladat ellátásához szükségük van.

8. Adatvédelmi incidens

8.1. Az adatkezelő a belső adatvédelmi felelős útján az adatvédelmi incidenssel kapcsolatos intézkedések ellenőrzése, valamint az érintett tájékoztatása céljából az 5. számú melléklet szerinti nyilvántartást vezet, amely 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.

8.2. Az érintett kérelmére az adatkezelő tájékoztatást ad az érintett általa kezelt, illetve az általa vagy rendelkezése szerint megbízott adatfeldolgozó által feldolgozott adatairól, azok forrásáról, az adatkezelés céljáról, jogalapjáról, időtartamáról, az adatfeldolgozó nevéről, címéről és az adatkezeléssel összefüggő tevékenységéről, az adatvédelmi incidens körülményeiről, hatásairól és az elhárítására megtett intézkedésekről, továbbá - az érintett személyes adatainak továbbítása esetén - az adattovábbítás jogalapjáról és címzettjéről.

9. A kiemelt védelem felelősei és tevékenységi köreik

9.1. Az adatbiztonság szabályozásának biztosítania kell:

a) az adatkezelésre használt számítástechnikai és manuális eszközökhöz történő illetéktelen fizikai hozzáférés megakadályozását,
b) annak megakadályozását, hogy az adatkezelésre használt számítástechnikai és manuális eszköztárba illetéktelenek bevitelt hajtsanak végre vagy a tár tartalmát illetéktelenül megismerjék, töröljék, vagy bármilyen módon megváltoztassák,
c) annak megakadályozását, hogy adatkezelésre használt távadat-átviteli vonalon az adatokhoz illetéktelenül hozzáférjenek,
d) a hozzáférési jogosultság betartását,
e) azoknak az azonosítását, akiknek az adatkezelésből adatokat továbbítanak,
f) annak azonosítását, hogy a számítástechnikai, valamint manuálisan vezetett eszköztárba milyen adatokat, mikor és ki rögzített, illetve intézkedett a rögzítésről,
g) annak megakadályozását, hogy az adatok továbbítása alkalmával az adatokat illetéktelenül megismerjék, lemásolják, töröljék vagy bármilyen módon megváltoztassák.

9.2. A fizikai biztonság szabályozásakor különösen fontosak az alábbi szempontok:

- az adattároló gépek helyiségét úgy kell kialakítani, hogy elegendő biztonságot nyújtsanak illetéktelen vagy erőszakos behatolás, tűz vagy természeti csapás ellen;
- a számítástechnikai szoftverek és programok hozzáférési kulcsát (azonosító kártya, jelszó) szolgálati titokként kell kezelni;
- gondoskodni kell arról, hogy a számítástechnikai eszközök biztonsági megoldásainak dokumentációjához csak az arra felhatalmazott személyek férjenek hozzá.

9.3. Az üzemeltetési biztonság szabályozásakor különösen fontosak az alábbi szempontok:

- össze kell állítani és elérhető helyen kell tartani a számítástechnikai eszközök használatára felhatalmazott személyek névsorát, feladataikat körül kell határolni;
- meg kell határozni az adatokhoz való hozzáférés szintjének szabályait;
- külső személy – pl. karbantartás, javítás, fejlesztés céljából – a számítástechnikai eszközökhöz lehetőleg úgy férjen hozzá, hogy a kezelt adatokat ne ismerje meg, amennyiben el elkerülhetetlen, adatvédelmi és titoktartási nyilatkozatot kell vele aláíratni
- a számítástechnikai rendszert – ideértve a programokat is – dokumentálni kell. A rendszer vagy annak bármely eleme csak a rendszergazda által változtatható meg a hozzáférés jelszavait időközönként, de az üzemeltető személyének megváltozásakor azzal egyidejűleg meg kell változtatni.
- a számítástechnikai rendszer üzemeltetéséről – hagyományos vagy automatikus módon – nyilvántartást kell vezetni, amelyet az arra illetékes személynek folyamatosan ellenőriznie kell;

- a hálózaton tárolt dokumentumokat úgy kell kezelni, hogy elvesztésük, elcserélésük vagy meghibásodásuk elkerülhető, kiküszöbölhető legyen;
- olyan tervet kell kidolgozni, amely a számítástechnikai eszközök előre nem látható üzemzavarának hatását ellensúlyozni képes intézkedéseket tartalmaz.

9.4. A technikai biztonság kiemelt szempontjai:

- az adatok és programok véletlen vagy szándékos megrongálását számítástechnikai módszerekkel is meg kell akadályozni;
- az adatállományok kezelését úgy kell megszervezni, hogy részleges vagy teljes megsemmisülésük esetén tartalmuk rekonstruálható legyen, az adatállományok tartalmát képező adattételek számát folyamatosan ellenőrizni kell;
- a hozzáférést jelszavakkal kell ellenőrizni;
- az adatok és az adatállományok változását naplózni kell;
- az adatbevitel során a bevitt adatok helyességét ellenőrizni kell;
- programfejlesztés vagy próba céljára valódi adatok felhasználását – ha a próbát külső szerv vagy személy végzi – el kell kerülni.

10. A Szabályzat alkalmazásának módja

A szabályzat megismerését az érintett köztisztviselők részére a jegyző biztosítja, az egyes munkaköri leírásoknak és a szabályzat előírásainak megfelelően.

10.1. A szabályzat karbantartása

A szabályzatot a vonatkozó jogi szabályozásban, informatikában, valamint a Hivatalban bekövetkező változások miatt időközönként aktualizálni kell. Ez a belső adatvédelmi felelős feladata, amelyhez az informatikai rendszer üzemeltetésével megbízott személy a számítástechnikai vonatkozások terén szakmai segítséget nyújt.

10.2. A védelmet igénylő adatok és információk osztályozása, minősítése, hozzáférési jogosultság

Az adatok kezelésére, illetve a számítógépes rendszer üzemeltetésével kapcsolatos feladatok ellátására felhatalmazott személyek az adatokhoz csak a feladatuk ellátásához szükséges mértékben, az alábbiak szerint férhetnek hozzá:

- A rendszerben adatkarbantartást csak az informatikusok végezhetnek. Az adatszolgáltatást igénybe vevő, illetve a nyilvántartást vezető vagy üzemeltető szerv más dolgozója az adatállományban változtatást nem végezhet. Az általa észlelt adathiba esetén erről a felhatalmazott köztisztviselőt értesíti, aki a kijavítás elvégzéséről intézkedik.
- A rendszerfejlesztők a feladataik ellátásához szükséges mértékig az adatállományokhoz hozzáférhetnek, az adatokat azonban nem használhatják fel más célra, és nem hozhatják mások tudomására.
- Az üzemeltető, illetve az adatszolgáltatást közvetlenül igénybe vevő szerv dolgozói csak meghatározott jelszó és azonosító használatával férhetnek hozzá az adatállományhoz, amelyek egyidejűleg meghatározzák az adathozzáférési jogosultság mértékét is.
- A rendszer üzemeltetői csak az adatállományok kezelésére, a nyilvántartás szervei által jelentett változások átvezetésére, a szolgáltatásokkal kapcsolatos technikai feladatok ellátására, a számítógépes rendszer működéséhez szükséges beavatkozások elvégzésére jogosultak. Az üzemeltető az adatállományban szereplő adatokat más, általa kezelt nyilvántartáshoz törvényi felhatalmazás nélkül nem használhatja fel.

10.3. A nyilvántartások összekapcsolása

A nyilvántartás más nyilvántartásokkal – ha törvény az adatkezelés céljának és az adatok körének pontos meghatározásával másképp nem rendelkezik – nem kapcsolható össze.

11. Védelmi eszközök és módszerek

11.1. Általános rendelkezések

11.1.1. Tűzvédelem

A kiszolgáló helyiség "D" tűzveszélyességi osztályba tartozik, amely mérsékelt tűzveszélyes üzemet jelent. A tűzvédelem feladatait, sajátos előírásokat a Hivatal Tűzvédelmi Szabályzata tartalmazza.

11.1.2. Vagyonvédelem, fizikai biztonság

- a helyiségeket biztonsági zárakkal kell felszerelni,
- a helyiségekbe való be- és kilépés rendjét szabályozni kell,
- munkaidőn túl a helyiségekben csak engedéllyel lehet tartózkodni,
- a helyiségekbe történő illetéktelen behatolás tényét a szervezet vezetőjének azonnal jelenteni kell,
- az irodahelyiségekben elhelyezett számítástechnikai eszközöket csak a kijelölt köztisztviselők használhatják,
- a számítástechnikai eszközök rendeltetésszerű működtetéséért a felhasználó felelős.

11.1.3. Adatvédelmi feladatok:

- az adatbevitel hibátlan műszaki állapotú berendezésen történjen,
- adatrögzítésre alkalmas szoftver védelme: a programokat és az adatokat ellenőrző funkciókkal, amennyiben szükséges titkosítással kell ellátni,
- a bejelentkezési azonosítók használatával kell szabályozni, hogy ki milyen hozzáférési szinten férhet hozzá a programokhoz és adatokhoz (alapelv: a tárolt adatokhoz csak az illetékes szervezeti egységek személyei férjenek hozzá),
- az adatok bevitele során alapelv: egyazon állomány rögzítését és ellenőrzését ugyanaz a személy nem végezheti.

Az adatállományok fájl-védelme során gondoskodni kell arról, hogy azok ne károsodjanak. A fontosabb fájlokról biztonsági másolatot kell készíteni.

11.1.4. Vírusvédelem

A munkaállomásokon és szervereken, folyamatos vírusvédelmet kell biztosítani. Vírusfertőzés okozta hiba gyanúja esetén azonnal szólni kell az illetékes szakembernek, informatikusnak. Amennyiben nincs erre lehetőség (pl. munkaidőn kívül), a feldolgozásban lévő adatokat el kell menteni, majd a programból kilépve a gépet ki kell kapcsolni. A gépet addig bekapcsolni nem szabad, amíg azt az arra illetékes szakember, informatikus meg nem vizsgálta. A vírusfertőzést azonnal jelenteni kell az informatikusoknak.

11.1.5. Szoftver védelem

Az üzemeltetésért felelős köztisztviselőnek biztosítani kell, hogy a rendszerszoftver naprakész állapotban legyen és a segédprogramok, programkönyvtárak mindig hozzáférhetők legyenek az illetékes felhasználók számára.

) Programhoz való hozzáférés, programvédelem:

A kezelés folyamán az illetéktelen hozzáférést ki kell zárni. Gondoskodni kell arról, hogy a tárolt programok, file-ok ne károsodjanak, a dokumentációban leírtaknak megfelelően működjenek.

b) A programokról nyilvántartást kell vezetni, amelynek az alábbi adatokat kell tartalmaznia:

a) a program azonosítója,

b) a program készítőjének neve,

c) a feldolgozási rendszer megnevezése.

- Programok megőrzése, nyilvántartása:

a) a programokról naprakész nyilvántartást kell vezetni,

b) a nyilvántartásból egyértelműen megállapíthatóak legyenek a program azonosítására és kezelésére vonatkozó adatok.

11.1.6. Hardver védelem

- A számítógépeket óvni kell folyadéktól, túlzott páratartalomtól és hőigénybevételtől,
- a számítógép közelében ételt és italt fogyasztani tilos,

- a szerver teremben klímaberendezés használata kötelező;
- szervereknél biztosítani kell a szünetmentes feszültségforrást,
- a számítógép-hálózat csatornáit külön kábelcsatornában kell vezetni,
- a fali csatlakozók megbontása szigorúan tilos,
- csak földelt aljzatokat lehet használni számítógép üzemeltetéséhez,
- a lengő kábeleket úgy kell elhelyezni, hogy azok balesetet ne okozhassanak, alapelv: sűrűn használt utat szabadon kell hagyni,
- a számítógépek belsejébe nyúlni, és ott bárminemű változtatást okozni tilos, csak az illetékes szakember, illetve a szervizek szakemberei nyúlhatnak bele.

11.2. A Hivatal további védelmi előírásai

11.2.1. A rendszerben adatkarbantartást csak a felelős vezető által erre felhatalmazott dolgozó végezhet az informatikusok közreműködésével. Az adatszolgáltatást igénybe vevő, illetve a nyilvántartást vezető vagy üzemeltető szerv más dolgozója az adatállományban változtatást nem végezhet. Az általa észlelt adathiba esetén erről a felhatalmazott köztisztviselőt értesíti, aki a kijavítás elvégzéséről intézkedik.

11.2.2. Számítástechnikai védelmi előírások:

- a számítógépeket csak jelszóval lehessen használni,
- rendszeresen frissített, aktív vírusvédelemmel kell ellátni,
- a feldolgozáshoz szükséges programok elindításához és az adatok hozzáféréséhez jogosultsági azonosító kell,
- a bizalmas adatállományokat és dokumentumokat titkosítani kell, a titkosítás végezhető az adott szoftverrel, vagy külső programmal is,
- a teljes anyagról havi mentéseket kell készíteni, ezeket a törvényekben meghatározott ideig kell megőrizni (pl. adótörvény, társadalombiztosítási törvény, számviteli törvény).

12. A belső adatvédelmi felelős

12.1. Az Infotörvény 24. § (1) bekezdése alapján megbízott belső adatvédelmi felelős a feladatkörén belül

a) konkrét ügyekben felmerülő igények alapján adatvédelmi kérdésekben segítséget nyújt a hivatal munkatársai részére,
b) kivizsgálja és intézi a hozzá érkező bejelentéseket,
c) tudomására jutott visszásság esetén hivatalon belül felhívja az érintett köztisztviselőt a jogosulatlan adatkezelés megszüntetésére,
d) elkészíti és felülvizsgálja az adatvédelmi és adatbiztonsági szabályzatot, jogszabályváltozás miatt vagy más fontos okból gondoskodik annak módosításáról, kiegészítéséről,
e) vezeti az adatvédelmi nyilvántartást,
f) a közérdekű adatok nyilvánosságával kapcsolatban szükség szerint közreműködik a közvélemény tájékoztatásában és a hasonló adatok megismerése iránti kérelmek teljesítésében
g) vezeti az adatvédelmi incidensek nyilvántartását

12.2. A hivatal valamennyi munkatársa köteles

a) az Infotörvény és az ágazati jogszabályok, valamint jelen szabályzat adatvédelmi előírásait megismerni és maradéktalanul betartani,
b) előzetesen egyeztetni az adatvédelmi felelőssel a személyes adatok kezelését érintő ügyekben, továbbá az adatvédelmi biztos közreműködését igénylő kérdésekben,
c) tájékoztatni a feladatkörében felmerült bármely adatvédelmi problémáról, esetleges állásfoglalásról vagy fejleményről,
d) észrevétel estén az adatkezeléssel kapcsolatosan feltárt visszásságot haladéktalanul megszünteti.

12.3. A belső adatvédelmi felelős megbízása az 1/3. számú melléklettel történik. A megbízás visszavonásig érvényes.

13. Záró rendelkezés

Jelen szabályzat 2018. 05. 18. napján lép hatályba, hatálybalépésével egyidejűleg hatályát veszti a korábbi adatvédelmi és adatbiztonsági szabályzat és valamennyi módosítása.

Pécel, 2018. 05. 17.

PÉCEL VÁROS JEGYZŐJE 1.

Tóth László
jegyző

1/a. melléklet

Adatszolgáltatást igénylő lap (vizuál regiszterből)

Igénylő szervezet, személy neve, címe: .....

Igénylő szervezet kapcsolattartójának neve (tel., e-mail):.....

Igénylés időpontja: .....

Az adatszolgáltatás kért módja: .....
levél: .....
fax: .....
online: .....

Igénylés, adatfelhasználás célja: .....

Igénylés jogalapja: .....
.....

Igényelt adatok fajtája (személyes, közérdekű):.....

A kért adatok: .....
.....

Engedélyezés időpontja: .....

Engedélyező aláírása: .....

Kijelentem, hogy a rendelkezésemre bocsátott adatokat kizárólag az adatigénylés céljának megfelelően használom fel, az adatvédelemre vonatkozó jogszabályokat mindenkor megtartom.

Adatigénylő aláírása

1/b. melléklet

Adatszolgáltatást igénylő lap (TSZR-ből)

Szolgáltatást igénylő szervezet, személy neve, címe: .....

Szolgáltatást igénylő szervezet kapcsolattartójának neve (tel., e-mail):.....

Igénylés időpontja: .....

Az adatszolgáltatás típusa: .....
Jegyz. típ.: .....
Iktatószáma: .....
Jellege: .....
Célja: .....

Engedélyezés:
Szolgáltatás:..... Kezdete. .....Vége: .....

Általános paraméterek:

Többes találat kiadható?
Adat. szolg. tiltó kiadható?
Konkrét passz.ok kiadható?

Családi állapot fedett?
Újsz. nyilv. 90 nap kiadható?
Adatszolgáltatási naplóból kiadható?

Megjegyzés:
.....
.....

Kijelentem, hogy a rendelkezésemre bocsátott adatokat kizárólag az adatigénylés céljának megfelelően használom fel, az adatvédelemre vonatkozó jogszabályokat mindenkor megtartom.

Adatigénylő aláírása

2. melléklet

Adattovábbítási nyilvántartás

Az adatkezelő nyilvántartási azonosítója	Adatszolgál-tatás ideje	Az adatszolgáltatás		Az adatszolgáltatást igénylő polgár, jogi személy vagy jogi személyiséggel nem rendelkező szervezet, illetve megbízottja vagy képviselője neve	Megjegyzés
		Célja	Jogalapja		

3. melléklet

Péceli Város Jegyzője
2119 Pécel, Kossuth tér 1.

MEGBÍZÁS

Péceli
Polgármesteri Hivatalnál

a belső adatvédelmi feladatok ellátásával megbízom

.....

Feladatát a helyi szabályzatban foglaltak szerint köteles ellátni. A megbízás visszavonásig érvényes.

Pécel,

jegyző

Tudomásul vettem: .....

4. melléklet

Nyilvántartás azokról a köztisztviselőkről, akik az eljárás során jogosultak az egyes okmány-nyilvántartások adataihoz hozzáférni

Az érintett köztisztviselő neve	Szervezeti egysége
1.	
2.	
3.	
4.	
5.	
...	

5. melléklet

Adatvédelmi incidensek nyilvántartása

Az incidens időpontja	Adatvédelmi incidens leírása	Az érintettek köre és száma	Az érintett személyes adatok/ nyilvántartások köre	Az incidens körülményei	Az incidens hatásai	Az incidens következményeinek csökkentésére és a hasonló incidensek jövőben történő elkerülése érdekében megtett intézkedések	A belső adatvédelmi felelős aláírása