ADATVÉDELMI ÉS ADATBIZTONSÁGI SZABÁLYZAT

Kübekháza Községi Önkormányzata, valamint Kübekházi Közös Önkormányzati Hivatala (a továbbiakban együtt: Adatkezelő) az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) 25/A. § (1) bekezdésében, valamint a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. törvény 30. § (1) bekezdésében kapott felhatalmazás alapján az általános adatvédelmi és adatbiztonsági szabályait az alábbiakban határozza meg.

Az Adatkezelő célja, hogy a tevékenységével összefüggésben felmerülő személyes adatok kezelésével járó folyamatai, eljárásai során biztosítsa a személyes adatok védelmének megfelelő szintjét az Európai Parlament és a Tanács 2016. április 27-i (EU) 2016/679 számú, a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről szóló rendelete szerint (a továbbiakban: általános adatvédelmi rendelet).

A szabályzatnak célja továbbá, hogy ismertesse az adatok kezelése során érvényesítendő szabályokat és eljárásokat mindazon személyekkel, akik az Adatkezelő adatvagyonához hozzáférhetnek az Adatkezelővel munkavégzésre, adatfeldolgozásra irányuló jogviszonyban állnak.

Az adatkezelési műveleteket az Adatkezelő úgy tervezi meg és hajtja végre, hogy az érintettek magánszférájának védelme megfelelő módon biztosított legyen. A technika mindenkori fejlettségére tekintettel megteszi azokat a technikai és szervezési intézkedéseket és kialakítja azokat az eljárási szabályokat, amelyek az adatbiztonság érvényre juttatásához szükségesek. Az adatokat védi különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, az adatok károsodása és véletlen elvesztése, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen.

I. Általános rendelkezések

1. § A szabályzat célja az Adatkezelő által végzett adatkezelések, adatfeldolgozások során a személyes adatok védelme és a közérdekű, illetve közérdekből nyilvános adatok hozzáférhetőségének biztosítása.

2. § A szabályzat tárgyi hatálya - figyelemmel az Infotv. 2. §-ában foglaltakra - kiterjed az Adatkezelő által folytatott minden olyan adatkezelésre és adatfeldolgozásra, amely természetes személy adataira vonatkozik, valamint amely közérdekű adatot vagy közérdekből nyilvános adatot tartalmaz, függetlenül attól, hogy az adatkezelés, adatfeldolgozás teljesen vagy részben automatizált eszközzel, vagy manuális módon történik.

3. § A szabályzat hatálya nem terjed ki:

a) az Adatkezelő információbiztonsági szabályzatában rendezett kérdésekre,

b) az Adatkezelő munkavégzésre irányuló jogviszonnyal kapcsolatos adatkezelési tevékenységére, csak amennyiben az ilyen tárgyú szabályzat e szabályzatra visszautal,

c) az anonim információkra, nevezetesen olyan információkra, amelyek nem azonosított vagy azonosítható természetes személyekre vonatkoznak, valamint az olyan személyes adatokra, amelyeket olyan módon anonimizáltak, amelynek következtében az érintett nem vagy többé nem azonosítható,

d) az elhunyt személyekkel kapcsolatos személyes adatok kezelésére.

4. § A szabályzat személyi hatálya kiterjed az önkormányzat tisztségviselőire, valamint a hivatal által foglalkoztatott valamennyi köztisztviselőre, ügykezelőre, munka törvénykönyve hatálya alátartozó munkavállalóra, munkavégzésre irányuló egyéb jogviszonyban álló személyre, továbbá az adatfeldolgozási szerződésekben rögzítettek szerint az adatfeldolgozási szerződést aláírt külső szervezetek mindazon alkalmazottaira, akik az Adatkezelő informatikai rendszereit használják, üzemeltetik, működtetik vagy fejlesztik - azaz mindazon személyekre, akik az Adatkezelő adatvagyonához hozzáférhetnek (a továbbiakban: alkalmazott).

5. § Az értelmező rendelkezések tekintetében az Infotv. 3. §-a az irányadó.

6. § A személyes adatok védelméhez fűződő jogot és az érintett személyiségi jogait, ha törvény kivételt nem tesz, az adatkezeléshez fűződő más érdekek - ideértve a közérdekű adatok nyilvánosságát is - nem sérthetik.

II. Az adatkezelési jogalapja és korlátai

7.§ Személyes adat főszabály szerint két esetben kezelhető:

a) ha az érintett hozzájárul az adatkezeléshez - ebben az esetben az Adatkezelőnél mindaddig, amíg az a személyes adatokat kezeli rendelkezésre kell állni az érintett kifejezett írásbeli hozzájáruló nyilatkozatának -,

b) vagy törvény vagy - törvényi felhatalmazás alapján, az abban meghatározott körben- helyi önkormányzat rendelete közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges adatkezelést rendel el,

c) további jogalapok:

1. 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,

2. az adatkezelés az Adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges,

3. az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges,

4. 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 (e pont a közhatalmi feladatellátáshoz kapcsolódó adatkezelés során nem alkalmazható).

8. § Különleges adatok kezelésével járó ügyekben a jelen szabályzatban foglaltakon túl is megkülönböztetett gondossággal kell eljárni. Figyelemmel kell lenni arra, hogy különleges adatok kizárólag törvényi (illetve az általános adatvédelmi rendeletbeli) felhatalmazás alapján, vagy az érintett írásbeli hozzájárulásával kezelhetőek.

9. § Az Adatkezelő adatkezelési tájékoztatással kapcsolatos kötelezettségei:

a) az újonnan megkezdett adatkezelés esetében

1. amennyiben az érintettre vonatkozó személyes adatokat az Adatkezelő az érintettől gyűjti, a személyes adatok megszerzésének időpontjában,

2. amennyiben az érintett utólag kér tájékoztatást, úgy ezen tájékoztatás megadásakor is

b) az érintett rendelkezésére kell bocsátani az alábbi információkat:

1. az Adatkezelő és - amennyiben ilyen kijelölésre kerül - képviselőjének kiléte és elérhetőségei,

2. az adatvédelemért felelős személy (községi önkormányzat esetén a polgármester, közös önkormányzati hivatal esetén a jegyző) elérhetőségei,

3. a személyes adatok tervezett kezelésének célja, valamint az adatkezelés jogalapja (ideértve különösen az Adatkezelő és harmadik fél jogos érdekeinek kifejtését is),

4. a személyes adatok címzettjei, amennyiben van ilyen, a címzettek kategóriái,

5. adott esetben annak a ténye, ha az Adatkezelő harmadik országba, vagy nemzetközi szervezet részére kívánja az adatokat továbbítani, a vonatkozó megfelelőségi határozat léte vagy hiánya, vagy ilyen adattovábbítás esetén megfelelő és alkalmas garanciák megjelölése, valamint azok másolatának megszerzésére szolgáló módokra vagy azok elérhetőségére való hivatkozás,

6. a személyes adatok tárolásának időtartama, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjai,

7. az érintett azon jogáról történő tájékoztatása, hogy kérelmezheti az Adatkezelőtől a rá vonatkozó személyes adatokhoz való hozzáférést, azok helyesbítését, törlését vagy kezelésének korlátozását (zárolás) és tiltakozhat az ilyen személyes adatok kezelése ellen, valamint az érintett adathordozhatósághoz való jogát,

8. amennyiben az adatkezelés az érintett hozzájárulásán alapul, az arról való tájékoztatást, hogy hozzájárulását bármely időpontban visszavonhatja, amely nem érinti a visszavonás előtt a hozzájárulás alapján végrehajtott adatkezelés jogszerűségét,

9. az érintettnek joga van felügyeleti hatósághoz címzett panasz benyújtására,

10. azt, hogy a személyes adat szolgáltatása jogszabályon vagy szerződéses kötelezettségen alapul vagy szerződés kötésének előfeltétele-e, valamint, hogy az érintett köteles-e személyes adatokat megadni, továbbá, hogy milyen lehetséges következményekkel járhat az adatszolgáltatás elmaradása,

11. amennyiben ez releváns, az automatizált döntéshozatal ténye, ideértve a profilalkotást is, valamint legalább ezekben az esetekben az alkalmazott logikára és arra vonatkozó közlés, hogy az ilyen adatkezelés milyen jelentőséggel és az érintettre nézve milyen várható következményekkel bír.

c) az újonnan megkezdett adatkezelés esetében amennyiben erre lehetőség van, továbbá, ha az érintettre vonatkozó személyes adatokat az Adatkezelő nem az érintettől gyűjti, a személyes adatok megszerzésének időpontjában, illetőleg a tájékoztató elkészítésekor az érintett rendelkezésére bocsátja a fenti információkat, valamint a személyes adatok forrását és adott esetben azt, hogy az adatok nyilvánosan hozzáférhető forrásból származnak-e.

10. § A személyes adatok kezelése célhoz kötöttségének elve alapján az egyes eljárások során kezelt adatokat csak az adott ügy elintézése érdekében szabad felhasználni, más eljárásokkal, illetve adatokkal azok nem kapcsolhatók össze, kivéve, ha törvény megengedi, illetve az érintett hozzájárult és az adatkezelés feltételei minden egyes személyes adatra vonatkozóan fennállnak.

11. § Konkrét ügyben hivatalból csak azokat a személyes adatokat lehet rögzíteni, amelyek kezelésére törvény vagy törvény felhatalmazása alapján, az abban meghatározott körben önkormányzati rendelet, illetve az érintett felhatalmazást ad, mellőzve a bemutatott személyazonosító és egyéb okmányok, személyes iratok indokolatlan fénymásolását és megőrzését.

12. § Amennyiben az Adatkezelő a személyes adatokon a gyűjtésük céljától eltérő további célból adatkezelést kíván végezni és erre lehetősége van, az általános adatvédelmi rendelet vonatkozó szabályaira tekintettel a további adatkezelést megelőzően tájékoztatja az érintettet erről az eltérő célról és minden, a fenti pontokban megfogalmazott információról.

13. § Az adatminőség biztosítása céljából az adatfelvétel és a további adatkezelés folyamán ügyelni kell a személyes adatok felvételének és kezelésének törvényességére, pontosságára, teljességére és - amennyiben az adatkezelés céljára tekintettel szükséges - időszerűségére, megfelelő tárolására, hogy emiatt az érintettek jogai ne sérülhessenek.

14. § A célhoz nem kötött és olyan adatokat, amelyekre nézve az adatkezelés célja megszűnt vagy módosult – az Adatkezelő Iratkezelési Szabályzatában (a továbbiakban: Iratkezelési Szabályzat) foglaltakkal összhangban - haladéktalanul, illetve az előírt megőrzési határidő leteltével meg kell semmisíteni. A személyes adatokat tartalmazó egyéb iratanyagok megsemmisítéséről szintén a szükséges biztonsági intézkedések mellett kell gondoskodni. Az elektronikus úton rögzített adatokat, ha céljukat betöltötték további felhasználásuk megakadályozása érdekében felismerhetetlenné, hozzáférhetetlenné kell tenni.

15. § Az adattörlés maradéktalan megvalósítása érdekében az irattározásra kerülő anyagok selejtezési idejét, irattári jelét az önkormányzati hivatalok egységes irattári tervének kiadásáról szóló 78/2012. (XII.28.) BM rendelet határozza meg.

16. § Adatkezelő továbbá törli vagy anonimizálja az érintettre vonatkozó, az informatikai rendszereiben, valamint papír alapú dokumentációiban szereplő személyes adatokat, ha jogszabály máshogy nem rendelkezik és a személyes adat kezeléséhez fűződő cél megszűnt. Ha a személyes adat törlése nem valósítható meg, az azt tartalmazó irat sérelme nélkül:

a) és az irat megőrzéséhez az Adatkezelő, vagy harmadik személy jogos érdeke fűződik, az iratot az Adatkezelő az iratkezelési szabályok szerinti időtartamig megőrzi, törlési kérelem esetén az iratot zártan kezeli és erről az érintettet értesíti, és az iratot a személyes adattal együtt az Iratkezelési Szabályzatban meghatározott időtartam lejártát követően megsemmisíti,

b) amennyiben az irat megőrzéséhez az Adatkezelőnek és harmadik személynek nem fűződik jogos érdeke, az iratot a személyes adattal együtt megsemmisíti.

17. § Az adatok törlése iránt minden esetben az adatvédelemért felelős személy a személyes adat kezelésével kapcsolatban érintett szervezeti egységgel, informatikai rendszer rendszergazdájával együttműködésben intézkedik. Az Adatkezelő informatikai rendszereiből a személyes adatot - az adott informatikai rendszer adottságai szerint - az élő rendszerből visszaállíthatatlanul törli vagy anonimizálja, továbbá az elérhető technológia és a megvalósítás költségeinek figyelembevételével megteszi az elvárható lépéseket és gondoskodik arról, hogy az informatikai rendszer archivált változatában is -a technológiai, technikai lehetőségek függvényében - átvezetésre kerüljön a személyes adat törlése. A törlésért az informatikai rendszerért felelős személy felel. Amennyiben a helyreállíthatatlan törlés az informatikai rendszer sajátosságából következő okból nem kivitelezhető, az Adatkezelő az adat logikai törlését hajtja végre. Az anonimizálás keretében a személyes adatot olyan azonosítóra kell lecserélni, amely megakadályozza, hogy a személyes adathoz tartozó további adatok a későbbiekben kapcsolatba hozhatók legyenek az érintettel. A papír alapú dokumentációk esetében azok jegyzőkönyvvel rögzített megsemmisítéséről kell gondoskodni. A jegyzőkönyvben rögzíteni kell: a megsemmisített iratok típusát, a megsemmisített iratok beazonosíthatóságához szükséges információkat, a megsemmisítés időpontját és a megsemmisítést végző személy nevét, beosztását, külső partner esetén a külső partner nevét.

18. § A személyes adatok akkor továbbíthatók, valamint a különböző adatkezelések akkor kapcsolhatók össze, ha az érintett ahhoz hozzájárult, vagy törvény azt megengedi, és ha az adatkezelés feltételei minden egyes személyes adatra nézve teljesülnek. Személyes adat (beleértve a különleges adatot is) az országból - az adathordozótól vagy az adatátvitel módjától függetlenül - harmadik országba, továbbá nemzetközi szervezet keretein belül adatkezelést folytató adatkezelő vagy adatfeldolgozó részére akkor továbbítható, ha az Infotv. 10. §-ában foglalt feltételek teljesülnek.

19. § A hatósági ügyek során hozott döntések nem tartalmazhatják az értesítendő személyek és szervek nevét, címét. Annak érdekében, hogy a kézbesítés ellenőrizhető legyen, a köztisztviselő köteles az irattári példányon rögzíteni az értesítendők jegyzékét, arról tájékoztatást adni azonban csak a vonatkozó jogszabályok és jelen szabályzat rendelkezéseinek figyelembevételével lehet.

III. Az érintett jogai

20. § Az érintettet a törvény szerint megilleti az a jog, hogy személyes adatai kezeléséről tájékoztatást kérjen.

A kérelmet (a jogszabályi feltételek fennállása esetén) a törvény alapján a legrövidebb idő alatt, de legfeljebb 25 napon belül elbírálja. A tájékoztatásnak az Infotv. 16. § (1)-(2) bekezdése szerinti adatokat kell tartalmaznia. A tájékoztatás ingyenes, ha a tájékoztatást kérő a folyó évben azonos adatkörre vonatkozóan tájékoztatási kérelmet még nem nyújtott be. Egyéb esetben a közérdekű adatok megismerésére irányuló igények teljesítésének rendjéről szóló szabályzatban meghatározott díjak az irányadók. A már megfizetett költségtérítést vissza kell téríteni, ha az adatokat jogellenesen kezelték vagy a tájékoztatás kérése helyesbítéshez vezetett.

A tájékoztatás az adott adatkezelésről készült tájékoztatóban megjelölt elektronikus e mail címen vagy postai levélben kérhető. A tájékoztatást az érintett által kért formában kell megadni, erre irányuló kifejezett kérés hiányában elsősorban elektronikus úton, másodsorban postai küldeményként kell megadni, amennyiben az Adatkezelő számára rendelkezésre áll a kommunikációs forma használatához szükséges adat és amennyiben az érintett személyazonossága kétséget kizáróan megállapítható.

A tájékoztatás keretében az adatvédelemért felelős személy - vagy a szerződésben erre a feladatra kijelölt adatfeldolgozó - köteles az érintettre vonatkozó, Adatkezelő által kezelt adatokról és a fentiekről tájékoztatást adni.

21. § Az Adatkezelő az érintett kérelmére köteles arra, hogy az érintettre vonatkozó személyes adatokat indokolatlan késedelem nélkül, de legfeljebb 25 napon belül törölje, ha az alábbi indokok valamelyike fennáll:

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

b) az érintett visszavonja az adatkezelés alapját szolgáló hozzájárulását és az adatkezelésnek más jogalapja nincs,

c) az érintett a közérdekű, valamint az Adatkezelő vagy harmadik fél jogos érdekeinek érvényesítéséhez szükséges adatkezelés ellen tiltakozik és nincs elsőbbséget élvező jogszerű ok az adatkezelésre, vagy az érintett a közvetlen üzletszerzés céljából beszerzett adatainak kezelése ellen tiltakozik,

d) a személyes adatokat jogellenesen kezelte az Adatkezelő,

e) a személyes adatokat az Adatkezelőre alkalmazandó uniós vagy tagállami jogban előírt jogi kötelezettség teljesítéséhez törölni kell,

f) a személyes adatok gyűjtésére az általános adatvédelmi rendelet szerinti, információs társadalommal összefüggő szolgáltatások kínálásával kapcsolatosan került sor.

22. § A törlést nem kell teljesíteni amennyiben az adatkezelés szükséges

a) a véleménynyilvánítás szabadságához vagy a tájékoztatáshoz való jog gyakorlása céljából,

b) a személyes adatok kezelését előíró, az adatkezelőre alkalmazandó uniós vagy tagállami jog szerinti kötelezettség teljesítése, illetve közérdekből vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlása keretében végzett feladat végrehajtása céljából,

c) az általános adatvédelmi rendeletben meghatározottak szerint a népegészségügy területét érintő közérdek alapján;

d) közérdekű archiválás, tudományos vagy történelmi kutatás, statisztikai célból és az adattörlés lehetetlenné tenné, vagy komolyan veszélyeztetné az adatkezelés céljának teljesítését,

e) jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez.

Amennyiben az adatok törlése jogszabályi előírás, de az az érintett jogos érdeke miatt nem lehetséges, a személyes adatot, illetve a személyes adatot tartalmazó elektronikus vagy papír alapú dokumentációt zárolni kell. Ez esetben az informatikai rendszerben tárolt adathoz, illetve dokumentumhoz csak az informatikai rendszer rendszergazdája vagy az adatvédelemért felelős személy rendelkezhet hozzáféréssel. Papír alapú dokumentációk esetén pedig a dokumentum őrzését zárható szekrényben kell megvalósítani. A papír alapú dokumentációk belső rendszerbe feltöltött elektronikus példányához az Adatkezelő a felhasználók hozzáférését megszünteti.

23. § Az érintett bármikor jogosult a helytelenül rögzített adatainak helyesbítését kémi. Amennyiben az érintett jelzi, hogy az Adatkezelő által kezelt bármely adata nem felel meg a valóságnak, az adatvédelemért felelős személy azonosítja az érintettet, valamint az általa helyesbítésre kért adat nyilvántartási helyét, és gondoskodik az adat helyesbítéséről, ezen eljárása keretében az adat helyesbítésére vonatkozó igényt az Adatkezelő érintett informatikai rendszerének rendszergazdája felé jelzi, a szükséges azonosító adatok, a hibás és a helyes adat megadásával. Amennyiben a helyes adat nem áll rendelkezésre, az adatvédelemért felelős személy az érintettől kér felvilágosítást a helyes adatról. Ha a helyes adat nem állapítható meg, az adatvédelemért felelős személy gondoskodik a helytelen adat zárolásáról. A zárolás az adat passzív állapotba helyezését jelenti, valamint értesíti az érintetett, hogy az adat helyesbítésére a helyes adat hiányában nincs mód, de az adat zárolásra került. Az eljárás határideje 30 nap.

24. § Az érintett jogosult arra, hogy tiltakozzon személyes adatának kezelése ellen. Az adatvédelemért felelős személy a legrövidebb időn belül azonosítja az érintettet, a tiltakozást a kérelem benyújtásától számított legrövidebb időn belül megvizsgálja, annak megalapozottsága kérdésében döntést hoz és döntéséről a kérelmezőt tájékoztatja.

25. § Az érintett jogosult arra, hogy kérésére az Adatkezelő korlátozza az adatkezelést, ha az alábbiak valamelyike teljesül:

a) ha az érintett vitatja az Adatkezelő, illetve a megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által kezelt személyes adatok pontosságát, helytállóságát vagy hiánytalanságát, és a kezelt személyes adatok pontossága, helytállósága vagy hiánytalansága kétséget kizáróan nem állapítható meg, a fennálló kétség tisztázásának időtartamára,

b) az adatkezelés jogellenes és emiatt az adatok törlésének lenne helye, de az érintett írásbeli nyilatkozata vagy az adatkezelő rendelkezésére álló információk alapján megalapozottan feltételezhető, hogy az adatok törlése sértené az érintett jogos érdekeit, a törlés mellőzését megalapozó jogos érdek fennállásának időtartamára,

c) az adatkezelés jogellenes és emiatt az adatok törlésének lenne helye, de az adatkezelő vagy más közfeladatot ellátó szerv által vagy részvételével végzett, jogszabályban meghatározott vizsgálatok vagy eljárások - így különösen büntetőeljárás - során az adatok bizonyítékként való megőrzése szükséges, ezen vizsgálat vagy eljárás végleges, illetve jogerős lezárásáig, vagy

d) az adatkezelés jogellenes és emiatt az adatok törlésének lenne helye, de a törvény szerinti dokumentációs kötelezettség teljesítése céljából az adatok megőrzése szükséges a kezelt adat törlését követő tíz évig.

Ha az adatkezelés korlátozás alá esik, az ilyen személyes adatokat a tárolás kivételével csak az érintett hozzájárulásával, vagy jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez, vagy más természetes vagy jogi személy jogainak védelme érdekében, vagy az Unió, illetve valamely tagállam fontos közérdekéből lehet kezelni.

Az Adatkezelő az érintettet, akinek a kérésére korlátozták az adatkezelést, az adatkezelés korlátozásának feloldásáról előzetesen tájékoztatja.

26. § A panaszok kezelésével kapcsolatban az adatvédelemért felelős személy számára tájékoztatást kötelesek adni a személyes adatok kezelésében részt vevő alkalmazottak.

27. § Ha az Adatkezelő bizonyítani tudja, hogy nincs abban a helyzetben, hogy azonosítsa az érintettet, erről lehetőség szerint őt megfelelő módon tájékoztatja. Ilyen esetekben az érintett hozzáférési jogát, a helyesbítés és törlés kérésének jogát, az adatkezelés korlátozásához való jogát, az ezekhez kapcsolódó értesítési jogot, valamint adathordozhatósághoz való jogot az Adatkezelő nem biztosítja, kivéve, ha az érintett abból a célból, hogy az említettek szerinti jogát gyakorolja, az azonosítását lehetővé tevő kiegészítő információkat nyújt.

IV. Az adatvédelmi tisztviselő

28. § Az adatvédelmi tisztviselőt az adatvédelmi jog és gyakorlat megfelelő szintű ismerete, valamint az e fejezetben említett feladatok ellátására való alkalmasság alapján kell kijelölni. Az Adatkezelő adatvédelmi tisztviselőjét a jegyző nevezi ki.

29. § Az adatvédelmi tisztviselő elektronikus elérhetőségét közzéteszi. Az adatvédelmi tisztviselőhöz bármely érintett fordulhat. Az adatvédelmi tisztviselő feladatait az adatkezelési műveletekhez fűződő kockázat megfelelő figyelembevételével, az adatkezelés jellegére, hatókörére, körülményére és céljára is tekintettel végzi. Az adatvédelmi tisztviselő:

a) a személyes adatok kezelésére vonatkozó jogi előírásokról naprakész tájékoztatást nyújt és azok érvényesítésének módjaival kapcsolatban tanácsot ad az Adatkezelő, az adatfeldolgozó és az azok által foglalkoztatott, az adatkezelési műveleteket végző személyek részére,

b) folyamatosan figyelemmel kíséri és ellenőrzi a személyes adatok kezelésére vonatkozó jogi előírások, így különösen a jogszabályok és belső adatvédelmi és adatbiztonsági szabályzatok érvényesülését, ennek keretei között az egyes adatkezelési műveletekhez kapcsolódó egyértelmű feladatmeghatározás, az adatkezelési műveletekben közreműködő foglalkoztatottak adatvédelmi

ismereteinek bővítése és tudatosságnövelése, valamint a rendszeres időközönként lefolytatandó vizsgálatok megvalósulását,

c) elősegíti az érintettet megillető jogok gyakorlását, így különösen kivizsgálja az érintettek panaszait és kezdeményezi az adatkezelőnél, illetve az adatfeldolgozónál a panasz orvoslásához szükséges intézkedések megtételét,

d) szakmai tanácsadással elősegíti és figyelemmel kíséri az adatvédelmi hatásvizsgálat lefolytatását,

e) együttműködik az adatkezelés jogszerűségével kapcsolatos eljárások lefolytatására jogosult szervekkel és személyekkel, így különösen kapcsolatot tart a Nemzeti Adatvédelmi és Információszabadság Hatósággal az előzetes konzultáció és a Hatóság által lefolytatott eljárások elősegítése érdekében,

f) közreműködik a belső adatvédelmi és adatbiztonsági szabályzat megalkotásában,

g) igény szerint tájékoztatja a jegyzőt a konkrét ügyek vagy jelentősebb soron kívüli feladatok végrehajtásáról, tapasztalatairól,

h) részt vesz az adatvédelmi tisztviselők konferenciáján,

i) az adatkezelések átláthatóságának biztosítása érdekében vezeti az adatkezelési tevékenységek nyilvántartását, amely tartalmazza legalább:

1. az adatkezelő nevét és elérhetőségét, valamint - ha van ilyen - a közös adatkezelőnek, az adatkezelő képviselőjének és az adatvédelmi tisztviselőnek a nevét és elérhetőségét,

2. az adatkezelés céljait,

3. az érintettek kategóriáinak, valamint a személyes adatok kategóriáinak ismertetését,

4. olyan címzettek kategóriáit, akikkel a személyes adatokat közlik vagy közölni fogják, ideértve a harmadik országbeli címzetteket vagy nemzetközi szervezeteket,

5. adott esetben a személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információkat, beleértve a harmadik ország vagy a nemzetközi szervezet azonosítását, valamint az általános adatvédelmi rendelet 49. cikk (1) bekezdésének második albekezdés szerinti továbbítás esetében a megfelelő garanciák leírását,

6. ha lehetséges, a különböző adatkategóriák törlésére előirányzott határidőket,

7. ha lehetséges, az általános adatvédelmi rendelet 32. cikk (1) bekezdésében említett technikai és szervezési intézkedések általános leírását.

j) az érintettek jogainak biztosítása körében:

az adatvédelmi tisztviselő hatékony eljárásokat dolgoz ki annak érdekében, hogy az érintettek egyszerűen tudják a jogaikat gyakorolni vagy az általuk észlelt jogsértés miatt bejelentést tenni,

k) eljár az adatkezeléssel kapcsolatban érkezett panaszok, bejelentések kivizsgálása során,

l) ha a panasz vagy bejelentés kivizsgálása arra okot adó körülményeket tárt fel, jogosult a panasztevő vagy bejelentő egyidejű tájékoztatása mellett adatvédelmi intézkedések megtételére, azok kezdeményezésére,

m) adatvédelmi és adatbiztonsági követelmények érvényesítése, azok megtartásának ellenőrzése körében folyamatosan ellenőrzi az adatkezelést meghatározó jelen szabályzat és egyéb vonatkozó jogszabályok, belső adatvédelmi és adatbiztonsági szabályzatok rendelkezéseinek és az adatbiztonsági követelményeknek a megtartását, ideértve feladatkörök kijelölését, az adatkezelési műveletekben résztvevő személyek tudatosság-növelését és képzését, valamint a kapcsolódó auditokat is,

n) az Adatkezelő adatkezelési tevékenységével összefüggő döntések meghozatalában való közreműködése körében:

1. figyelemmel kíséri a jogszabályi rendelkezések gyakorlati alkalmazhatóságát, szükség esetén javaslatot tesz az egyes adatkezelési körülmények megváltoztatására vagy kiegészítésére,

2. közreműködik a szükséges jogszabály-módosítások előkészítésében,

3. az adatkezelést érintő döntés meghozatalát megelőzően véleményt nyilvánít tervezett döntéssel kapcsolatban. (Az ilyen döntés tekintetében kötelező a véleményének kikérése, amellyel egyidejűleg tájékoztatni kell legalább a döntés körülményeiről, hatásáról, döntési alternatívákról. A tájékoztatást olyan időben kell az adatvédelmi tisztviselő részére eljuttatni, hogy megfelelő idő álljon rendelkezésére álláspontja kialakítására. Az adatvédelmi tisztviselő a döntéssel kapcsolatos álláspontját a döntés meghozatalát megelőzően juttatja el a döntés előkészítőinek. A döntéshozatal során az adatvédelmi tisztviselő véleményét figyelembe kell venni),

o) az adatbiztonsági incidensek kezelése során a jelen szabályzat 51. §-ában foglaltak szerint jár el,

p) adatvédelmi ismeretek oktatása, terjesztése körében:

1. vezető tisztségviselők, alkalmazottak részére az adatvédelemmel kapcsolatos feladataikra és kötelezettségeikre kiterjedő rendszeres oktatást szervez, az általános adatvédelmi rendelet által meghatározott kötelezettségekkel kapcsolatban tájékoztatást, illetve szakmai tanácsot ad,

2. az Adatkezelő adatkezelésével kapcsolatos gyakorlat megváltozása esetén az tájékoztatást ad mindazok részére, akikre a változás hatással lehet,

3. gondoskodik az adatkezelést végző munkatársak adatvédelmi ismereteinek naprakészen tartásáról,

4. kérésre szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, valamint nyomon követi a hatásvizsgálatnak az általános adatvédelmi rendelet 35. cikkében foglaltak szerinti elvégzését.

V. Adatfeldolgozó igénybevétele

30. § Az Adatkezelő adatfeldolgozó igénybevétele esetén gondoskodik arról, hogy a kiválasztott adatfeldolgozó a személyes adatok védelme érdekében megtegye a szükséges intézkedéseket, valamint kövesse Adatkezelő szabályzatait és egyedi utasításait. A kiválasztás során az Adatkezelő törekszik arra, hogy csakis olyan adatfeldolgozó kerüljön igénybevételre, amely megfelelő garanciákat nyújt - különösen szakértelem, megbízhatóság és erőforrások tekintetében - arra vonatkozóan, hogy az adatvédelmi követelmények teljesülését biztosító technikai és szervezési intézkedéseket végrehajtja, ideértve az adatkezelés biztonságát is.

31. § A szabályzat hatálybalépését követően kötött adatfeldolgozói szerződésekben legalább az alábbiakról rendelkezni kell:

a) szerződés tárgya,

b) az Adatkezelő és az adatfeldolgozó adatai,

c) a feldolgozott adatok körének megjelölése,

d) az adatfeldolgozás céljai,

e) az adatfeldolgozás időtartama,

f) az adatkezelés jellege, típusa,

g) az érintettek köre,

h) adatfeldolgozó által ellátandó feladatok pontos leírása,

i) az írásbeli utasításhoz kötöttség ténye,

j) a tájékoztatási kötelezettség,

k) arról, hogy az adatfeldolgozó az általános adatvédelmi rendeletben alkalmazott biztonsági eljárásokra (álnevesítés, titkosítás) felkészült,

l) az Adatkezelő adatvédelemért felelős személyének elérhetősége,

m) adatfeldolgozó titoktartási kötelezettsége,

n) az adatfeldolgozó részéről adatkezelés jellegének figyelembevételével megfelelő technikai és szervezési intézkedések, valamint az adatbiztonsági előírások végrehajtásának vállalása,

o) annak meghatározása, hogy az adatfeldolgozónak az Adatkezelő mely szabályzatainak kell megfelelnie,

p) további adatfeldolgozó igénybevételének lehetősége, amennyiben ez ismert, a további adatfeldolgozó személyének megjelölésével, amennyiben nem ismert a bevonás menetére vonatkozó rendelkezéseket és az Adatkezelő ellenvetési jogát,

q) az adatfeldolgozás befejezését követő eljárásokat (minden személyes adatot törölni kell vagy vissza kell juttatni az Adatkezelő számára és törölni kell a meglévő másolatokat, kivéve, ha az uniós vagy a tagállami jog a személyes adatok tárolását írja elő),

r) azon kötelezettséget, hogy további adatfeldolgozó igénybevétele esetén az adatfeldolgozónak az eredeti szerződésének megfelelő tartalmú szerződést kell vele kötnie,

s) az együttműködés elvét, amely szerint az adatfeldolgozónak kötelessége az Adatkezelővel az adatkezelés során együttműködni,

t) azon kötelezettséget, hogy az Adatkezelő az adatfeldolgozó rendelkezésére bocsát minden olyan információt, amely az Adatkezelő általános adatvédelmi rendeletben megfogalmazott kötelezettségeinek teljesítéséhez szükséges,

u) az audit jog kikötése, amely szerint az adatfeldolgozó köteles elősegíteni az Adatkezelő által vagy az általa megbízott más természetes vagy jogi személy által végzett auditokat, beleértve a helyszíni ellenőrzéseket.

VI. Adatbiztonsági rendelkezések

Általános szabályok

32. § Valamennyi alkalmazott köteles:

a) az általános adatvédelmi rendelet, az Infotv. és az ágazati jogszabályok, valamint jelen szabályzat adatvédelmi előírásait megismerni és betartani,

b) indokolt esetben előzetesen egyeztetni az adatvédelmi felelőssel a személyes adatok kezelését vagy a közérdekű adatok nyilvánosságát érintő ügyekben, tájékoztatni a feladatkörében felmerült bármely egyéb ágazati adatvédelmi problémáról, esetleges állásfoglalásról vagy más fejleményről, észrevételezés esetén az adatkezeléssel kapcsolatosan feltárt visszásságot jelezni.

A munkavégzés szabályai

33. § Az alkalmazottak irodai helyiségüket és az irat és adattárolásra használt berendezéseket munkaidőben fokozott gondossággal kötelesek őrizni. Az alkalmazott köteles a számítógépét és az ahhoz alkalmazott adathordozókat úgy kezelni, tárolni, hogy a védelmet igénylő adatokat illetéktelen személy ne ismerhesse meg. Köteles továbbá a munkaidő végeztével a számítógépet kikapcsolni, az irodahelyiség ajtaját bezárni és a kulcsot a portaszolgálathoz leadni.

34. § Személyes adatokat is tartalmazó iratot vagy más adathordozót (a továbbiakban együtt: irat) az Adatkezelő helyiségeiből kivinni - munkaköri feladat ellátásának kivételével csak indokolt esetben, a felettes vezető egyetértésével lehet. Az alkalmazott ez esetben is köteles gondoskodni arról, hogy az irat ne vesszen el, ne rongálódjon vagy semmisüljön meg és tartalma illetéktelen személy tudomására ne jusson.

35. § Az alkalmazott a nála lévő iratokat köteles munkaidőn túl - és amelyeket lehetséges munkaidőben is - elzárt helyen tartani. Munkaidőben iratok csak a munkavégzés céljából és a munkavégzéshez szükséges időtartamban lehetnek a köztisztviselőnél.

36. § A képviselő testületi és bizottsági jegyzőkönyvek közül a zárt ülések jegyzőkönyveit fokozott gondossággal kell kezelni. A zárt ülések jegyzőkönyveit külön kell lefűzni vagy beköttetni, zárható szekrényben kell tárolni.

37. § Akár alkalmazottnál, akár irattárban lévő iratba az ügyintéző alkalmazotton kívül más személy - a vonatkozó eljárásjogi szabályok szerint - csak akkor tekinthet be, ha ezt jogszabály lehetővé teszi. A betekintési jog gyakorlása során úgy kell eljárni, hogy ez által mások személyes adatainak védelméhez fűződő jogai, illetve személyiségi jogai ne sérülhessenek. Jelen § rendelkezéseit kell alkalmazni a másolat, kivonat készítésekor is.

38. § Az ügyfélfogadáshoz az alkalmazottak részére lehetőség szerint külön szobát kell biztosítani. Külön szoba hiányában is az ügyfélfogadást úgy kell megszervezni, hogy annak megtartása ne járjon a személyes adatok védelméhez fűződő jog veszélyeztetésével, illetve sérelmével.

39. § Az egyes nyilvántartások, adatkezelések tekintetében a hozzáférési jogosultságot az illetékes szervezeti egység vezetőjének személyre szólóan meg kell határoznia és az időszerű állapotnak megfelelően a rendszergazdának nyilván kell tartania Adatkezelő információbiztonsági szabályzatában foglaltak szerint.

40. § Az alkalmazottak a munkavégzés, illetve feladatellátás során keletkezett személyes adatot is tartalmazó elektronikus dokumentumokat csak a munkavégzés céljára szolgáló számítástechnikai eszközökön nyithatják meg. Követelmény továbbá, hogy

a) a munkavégzésre, illetve feladatellátásra használt eszközt, amelyen az Adatkezelő által kezelt vagy feldolgozott személyes adat is megtalálható, minden esetben ábrás, vagy kódos védelemmel kell használni (Az alkalmazott köteles a munkáltató által biztosított készüléken képernyőzárat - ábrát vagy kódot - létrehozni, továbbá a készüléket folyamatosan ábrás vagy kódos védelemmel ellátva használni, melyet kizárólag az alkalmazott ismer. A hozzáférési kódokat az alkalmazottak bizalmasan kötelesek kezelni. Az alkalmazott köteles a kódot az eszköz visszaadásának napján az Adatkezelő számara megadni vagy az eszközt kóddal nem védett állapotban visszaszolgáltatni.),

b) a munkavégzés/feladatellátás céljára szolgáló eszközökön a személyes adatot is tartalmazó dokumentumot az alkalmazottak nem nyithatják meg. (Amennyiben valamely okból ez elkerülhetetlen, akkor a helyi másolatot minden esetben törölni kell az eszközről.),

c) a munkavégzés, illetve feladatellátás céljára átadott eszközöket kizárólag az alkalmazottak használhatják, hozzátartozóik vagy más személy számára nem engedélyezett a használat.

Személyes adatok kezelésére vonatkozó különös rendelkezések

41. § A papír alapú, személyes adatokat tartalmazó munkadokumentumokat olyan módon kell kezelni, tárolni, hogy azokhoz csak az erre a feladatra megbízott alkalmazott férhessen hozzá.

42. § Ha a papír alapú, személyes adatokat tartalmazó munkadokumentumok használata már nem szükséges, azokat olyan módon kell megsemmisíteni (pl.: irat ledarálásával), hogy a megsemmisítést követően ne lehessen a tartalmukat megállapítani.

43. § Tilos magánhasználatú eszközön az Adatkezelő kezelésében vagy feldolgozásában lévő személyes adatot tárolni, kivéve, ha a tárolás a munkavégzéshez elengedhetetlenül szükséges és a tárolást a munkavégzést követően megszüntetik.

44. § Az alkalmazott feladatellátásra szolgáló jogviszonya megszűnése esetén minden személyes adatot tartalmazó papír alapú és elektronikus iratot, adatot köteles a foglalkoztatásának utolsó napját megelőzően az Adatkezelő részére visszaszolgáltatni, azokról másolatot nem tarthat magánál. A visszaszolgáltatásról átadás-átvételi jegyzőkönyvet kell készíteni.

45. § Minden alkalmazott köteles a feladatellátására szolgáló munkaterületet olyan módon használni, hogy ott az Adatkezelő kezelésében vagy feldolgozásában lévő, személyes adatot is tartalmazó dokumentumok lehetőség szerint ne legyenek szabadon hozzáférhetők. Ilyen intézkedésnek minősül különösen: számítástechnikai eszközök jelszavas védelme, az irodahelyiség zárása, az iratok elhelyezése védett helyre. Adatkezelő minden munkatársa köteles biztosítani és megfelelő intézkedéseket megtenni annak érdekében, hogy az Adatkezelő hivatali és egyéb helyiségeibe az Adatkezelővel feladatvégzésre irányuló jogviszonyban nem álló személy csak alkalmazott kíséretében léphessen be. Az Adatkezelő helyiségeibe belépni jogosult személyek az Adatkezelő által kezelt személyes adatok megismerésére nem minden esetben jogosultak. Az alkalmazottak kötelesek megtenni mindent annak érdekében, hogy az Adatkezelő kezelésében álló személyes adatok biztonságban legyenek, az ennek megsértéséből az Adatkezelőt ért kárért az adatvédelmi incidenst előidéző személy felelősséggel tartozik.

46. § Személyes adatok csak biztonságos kommunikációs csatorna alkalmazásával, illetve megfelelő titkosítási megoldással adhatók át más személynek. Ellenkező jelzésig az Adatkezelő belső levelezési rendszerén belüli adatáramlás biztonságos kézbesítési csatornának tekintendő. Külső adatátadás során gondoskodni kell a személyes adatok titkosításáról SSL-kapcsolat, vagy egyedi titkosítás használatával, a jelszó elkülönített csatornán (pl.: SMS) keresztüli küldésével, papír alapon pedig zárt borítékon keresztüli átadással.

47. § Amennyiben az Adatkezelő más adatkezelőtől, az adathoz kapcsolódó rendelkezéssel fogad személyes adatot, valamennyi, az adattal érintkező felhasználónak kötelessége az adattovábbító rendelkezéseit figyelembe venni.

48. § Harmadik személynek titoktartási nyilatkozat hiányában személyes adat nem adható ki.

VII. Adatvédelmi incidensekkel kapcsolatos kötelezettségek

49. § Adatvédelmi incidens alatt az általános adatvédelmi rendelet értelmében a biztonság olyan sérülését értjük, 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.

50. § Az adatvédelmi incidens megfelelő és kellő idejű intézkedés hiányában fizikai, vagyoni vagy nem vagyoni károkat okozhat a természetes személyeknek, többek között a személyes adataik feletti rendelkezés elvesztését vagy a jogaik korlátozását, hátrányos megkülönböztetést, személyazonosság-lopást vagy személyazonossággal való visszaélést, pénzügyi veszteséget, álnevesítés engedély nélküli feloldását, jó hírnév sérelmét, szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülését, illetve egyéb jelentős gazdasági vagy szociális hátrányt. Ezért a jelen szabályzat hatálya alá tartozó személyek, bármely az Adatkezelő által vagy közreműködésével működtetett informatikai rendszer vagy manuális adatkezelés esetében haladéktalanul, de legkésőbb 24 órán belül kötelesek jelenteni az adatvédelmi tisztviselő számára, ha adatvédelmi incidens gyanúja merül fel, vagy ha tudomása van arról, hogy adatvédelmi incidens történt.

A bejelentést elsősorban munkaidőben, telefonon keresztül kell megtenni, és azt követően az adatvédelemért felelős személy számára küldött elektronikus levél formájában is meg kell erősíteni.

51. § Az adatvédelmi tisztviselő és az egyéb érintett személyek a számukra jelzett, vagy saját feladat- vagy hatáskörükben megállapított adatvédelmi incidens felderítése és súlyosságának megállapítása érdekében a jelen §-ban foglalt eljárásrend szerint kötelesek eljárni.

a) Adatkezelő minden szükséges intézkedést megtesz az adatvédelmi incidensek elkerülése érdekében.

b) Amennyiben mégis adatvédelmi incidens következik be az adatvédelmi tisztviselő felveszi a kapcsolatot az adatvédelmi incidenssel érintett informatikai rendszer rendszergazdájával, az adatvédelmi incidenssel érintett adatkezelési folyamat adatgazdájával, és ha azonosítható ilyen, az incidenst előidéző személlyel.

c) Az adatvédelmi tisztviselőnek a felderítés során az alábbi kategóriák valamelyikébe kell az adatvédelmi incidenst sorolni:

1. alacsony szintű adatvédelmi incidens: a személyes adatok elhanyagolható körének jogosulatlan továbbítása, megváltoztatása, nyilvánosságra hozatala, szándékolt, vagy véletlen törlése vagy megsemmisítése, vagy más jogellenes adatkezelési eset,

2. közepes szintű adatvédelmi incidens: a személyes adatok csekély körének megváltoztatása, jogosulatlan továbbítása, nyilvánosságra hozatala, szándékolt, vagy véletlen törlése vagy megsemmisítése, vagy más jogellenes adatkezelési eset,

3. magas szintű adatvédelmi incidens: a személyes adatok széles körének jogosulatlan megváltoztatása, továbbítása, nyilvánosságra hozatala, szándékolt, vagy véletlen törlése vagy megsemmisítése, vagy más jogellenes adatkezelési eset, illetve az adatok körétől függetlenül minden olyan eset, amikor valószínűsíthető, hogy az incidensnek az érintettre hátrányos hatása van, vagy biztosra vehető, hogy az incidensnek az érintettre hátrányos hatása van.

d) Adatvédelmi incidens megállapítása esetén megteendő intézkedések:

1. Alacsony szintű adatvédelmi incidens esetén az adatvédelmi tisztviselő:

1.1. legkésőbb a tudomásszerzéstől számított 2 napon belül az érintett rendszer rendszergazdájával és az adatvédelmi incidenssel érintett adatkezelési folyamat

adatgazdájával meghatározza az adatvédelmi incidens kezelésének módját és felhívja az intézkedésre jogosult személyt az incidens kezelésére,

1.2. rögzíti az adatvédelmi incidenst az incidensek nyilvántartásába.

2. Közepes szintű adatvédelmi incidens esetén az adatvédelmi tisztviselő:

2.1. haladéktalanul, de legkésőbb a tudomásszerzéstől számított 24 órán belül munkacsoportot hív össze, amelyben részt vesz az adatvédelemért felelős személyen kívül a rendszergazda, az adatvédelmi incidenssel érintett adatkezelési folyamat adatgazdája és Adatkezelő vezetője,

2.2. rögzíti az adatvédelmi incidenst az incidensek nyilvántartásában,

2.3. hetvenkét órán belül értesíti a felügyeleti hatóságot adatvédelmi incidensről,

2.4. ha az adatvédelmi incidens valószínűsíthetően kockázattal jár az érintett vagy más érintettek jogaira és szabadságaira nézve és a munkacsoport meghatározza az adatvédelmi incidens kezelésének módját, felhívja az intézkedésre jogosult személyt az incidens kezelésére.

3. Magas szintű adatvédelmi incidens esetén:

3.1. az adatvédelmi tisztviselő haladéktalanul, de legkésőbb a tudomásszerzéstől számított 24 órán belül munkacsoportot hív össze, amelyben részt vesz az adatvédelmi tisztviselő kívül a rendszergazda, az adatvédelmi incidenssel érintett adatkezelési folyamat adatgazdája és Adatkezelő vezetője,

3.2. a munkacsoport meghatározza az adatvédelmi incidens kezelésének módját és felhívja az intézkedésre jogosult személyt az incidens kezelésére, továbbá meghatározza az érintettek értesítésének módját, az értesítés tartalmát, és gondoskodik az érintettek haladéktalan értesítéséről,

3.3. az adatvédelmi tisztviselő rögzíti az adatvédelmi incidenst az incidensek nyilvántartásában,

3.4. az adatvédelmi tisztviselő a tudomásszerzéstől számított hetvenkét órán belül értesíti a felügyeleti hatóságot az adatvédelmi incidensről.

e) Az adatvédelmi tisztviselő az adatvédelmi incidenssel kapcsolatos intézkedések ellenőrzése, valamint az érintett tájékoztatása céljából az adatvédelmi incidensekről - az 1. melléklet szerinti tartalommal - nyilvántartást vezet.

f) Amennyiben az érintett kéri, az adatvédelmi tisztviselő tájékoztatást ad az érintett személyes adatát érintő adatvédelmi incidensről. Adatkezelő nem köteles tájékoztatni az érintettet az adatvédelmi incidensről, ha

1. az Adatkezelő megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre, és ezeket az intézkedéseket az adatvédelmi incidens által érintett adatok tekintetében alkalmazta (különösen azokat az intézkedéseket - mint például a titkosítás alkalmazása -, amelyek a

személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik az adatokat),

2. 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,

3. a tájékoztatás aránytalan erőfeszítést tenne szükségessé az Adatkezelő részéről. Ilyen esetekben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, vagy olyan hasonló intézkedést kell hozni, amely biztosítja az érintettek hasonlóan hatékony tájékoztatását (pl. sajtóközlemény kiadása).

g) Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az Adatkezelő indokolatlan késedelem nélkül köteles írásban, vagy ha rendelkezésre áll e-mail cím, akkor e-mailben tájékoztatni az érintettet az adatvédelmi incidensről. A tájékoztatásban világosan és közérthetően ismertetni kell az adatvédelmi incidens jellegét, és közölni kell legalább az alábbi információkat:

1. az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit,

2. az adatvédelmi incidensből eredő, valószínűsíthető következményeket,

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

52. § Az adatfeldolgozónál bekövetkező adatvédelmi incidensre irányadó szabályok:

a) ha az adatfeldolgozó rendszerében észlel adatvédelmi incidenst, indokolatlan késedelem nélkül köteles bejelenteni azt Adatkezelőnek, illetve amennyiben nem lehetséges az információkat egyidejűleg közölni, azokat köteles további indokolatlan késedelem nélkül akár részletekben is közölni,

b) amennyiben Adatkezelő észlel adatvédelmi incidenst valamely adatfeldolgozójánál, vagy adatvédelmi incidens gyanúja merül fel, akkor Adatkezelő az Adatfeldolgozó egyidejű értesítésével lefolytatja az adatvédelmi incidens azonosításával és kezelésével kapcsolatos, jelen fejezet szerinti eljárását,

c) az adatfeldolgozó - az adatfeldolgozási szerződésben foglalt kötelezettsége szerint - az Adatkezelővel egyeztetve köteles az incidens kezelésében együttműködni, illetve köteles minden olyan megfelelő technikai és szervezési intézkedéseket végrehajtani, ami a hasonló, vagy ugyanolyan adatvédelmi incidens elkerülése érdekében szükséges, és az incidens ismételt bekövetkezésének lehetőségét kizárja,

d) az adatvédelmi incidens bejelentésének elmaradásából, az incidens nem megfelelő kezeléséből és az együttműködési kötelezettség megszegéséből fakadó felelősség az adatfeldolgozót terheli.

VIII. Új adatkezelési tevékenység

53. § Személyes adatok kezelésével járó új tevékenységek bevezetésekor az alábbi feladatokat kell elvégeznie az adatvédelemért felelős személynek:

a) meg kell határoznia

1. a kezelendő személyes adatok körét,

2. az adatok kezelésének célját,

3. az adatkezelés jogalapját,

4. az adatkezelés időtartamát

b) fel kell mérnie, hogy az adatok milyen informatikai rendszerben lesznek kezelve,

c) meg kell határoznia, hogy előreláthatóan az adatokhoz kinek szükséges hozzáférnie az Adatkezelőnél, illetve rajta kívülálló külső szervnél, személynél,

d) be kell mutatni, hogy az adatokat szükséges-e továbbítani más személy számára,

e) be kell mutatni, hogy az adatkezeléshez igénybe kell-e venni adatfeldolgozót, amennyiben igen, az adatfeldolgozó feladata mi lesz, várhatóan ki lesz az adatfeldolgozó,

f) meg kell határozni az adatkezelés megkezdésének tervezett időpontját, az adatok felvételének módját és pontos helyét (pl.: erre szolgáló internetes felület vagy papír alapú adatfelvétel).

54. § A kialakított adatkezelési terv alapján az adatkezelésről szóló tájékoztatót és a végleges adatfeldolgozási szerződést az adatvédelmi tisztviselő készíti el.

IX. Záró rendelkezések

55. § Amennyiben a bíróság, a Nemzeti Adatvédelmi és Információszabadság Hatóság az Adatkezelőt személyes adatok jogsértő kezelése miatt elmarasztalja vagy kártérítésre kötelezi, az az érintett alkalmazott anyagi, fegyelmi, illetve büntetőjogi felelősségre vonását alapozza meg.

56. § Jelen szabályzat 2025. február 10. napján lép hatályba.

Kübekháza, 2025. február 7.

dr. Pungor Edit polgármester	**Kocsis Nóra Magdolna** jegyző

Adatvédelmi incidensek nyilvántartása

Az adatvédelmi incidens iktatószáma	Időpontja	Észlelés/Megállapítás időpontja	Bejelentés időpontja, ha késedelmesen vagy nem történt, annak oka	Az érintettek köre és száma	Az érintett személyes adatok köre	Bejelentés esetén a NAIH megállapítása, hogy incidens köre történt-e (I/N)	Az adatvédelmi incidens körülményei, hatásai	Az orvoslásra, további hasonló incidensek elkerülésére megtett intézkedések