SZIHALOM KÖZSÉGI ÖNKORMÁNYZAT ADATVÉDELMI ÉS ADATKEZELÉSI SZABÁLYZATÁRÓL

A jogalkotásról szóló 2010. évi CXXX. törvény 23.§ (4) bekezdésének j) pontjában biztosított felhatalmazás alapján az információbiztonságról szóló 2011. évi CXII. törvény 25/A.§ (3) bekezdésében foglalt feladatkörömben eljárva Szihalom Községi Önkormányzat adatvédelmi és adatbiztonsági szabályzatát az utasítás melléklete szerinti tartalommal adom ki.

Az utasítás 2020. szeptember 01. napján lép hatályba.

Szihalom, 2020. szeptember 01.

Szihalom Községi Önkormányzat

Bóta József Sándor
polgármester

SZIHALOM KÖZSÉGI ÖNKORMÁNYZAT ADATVÉDELMI ÉS ADATKEZELÉSI SZABÁLYZATA

I. BEVEZETŐ RENDELKEZÉSEK

1. A SZABÁLYZAT CÉLJA

E szabályzat megalkotásának és közzétételének célja az Európai Parlament és a Tanács (EU) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről szóló 2016/679 rendeletének történő megfelelés biztosítása, így különösen

1. a jogszabályban meghatározott **érintetti tájékoztatáshoz való jog megvalósulása**, azaz annak a követelmények az érvényesítése, hogy az érintettek megfelelő tájékoztatást kaphassanak
   a) az adatkezelő által kezelt, illetve az általa megbízott adatfeldolgozó által feldolgozott adatokról,
   b) azok forrásáról,
   c) az adatkezelés céljáról, jogalapjáról, időtartamáról,
   d) az adatkezelésbe esetlegesen bevont adatfeldolgozó nevéről, címéről és az adatkezeléssel összefüggő tevékenységéről, továbbá - az érintett személyes adatainak továbbítása esetén –
   e) az adattovábbítás jogalapjáról és címzettjéről.
2. az **adatvédelmi alapelvek** a szervezetnél történő **érvényesülésének meghatározása**,
3. az **incidenskezelési rendszer** meghatározása,
4. az adatkezelő **adatvédelmi rendszerének** bemutatása,
5. az **adatbiztonsági rendelkezések** meghatározása.

2. A SZABÁLYZAT HATÁLYA ÉS AZ ADATKEZELŐRE VONATKOZÓ ALAPVETŐ INFORMÁCIÓK

2.1. A szabályzat hatálya

E szabályzat **szervi hatálya**

Szihalom Községi Önkormányzatra (a továbbiakban: az Adatkezelő)

15729442-2-10 (adószám)

729446 (törzsszám)

3377 Szihalom, Hunyadi út 78. (székhely)

terjed ki.

A szabályzat tárgyi hatálya az Adatkezelő minden szervezeti egységénél és tevékenységi helyén folytatott valamennyi olyan folyamatára kiterjed, amely során a jogszabályban meghatározott, e fejezet 4. pontjában meghatározottak szerinti **személyes adat kezelése valósul meg.**

2.2. Az Adatkezelőre vonatkozó alapvető adatok:

Adatkezelő tevékenységi helyei:	**3377 Szihalom, Hunyadi út 78. (hivatali épület)**
	.....
Adatkezelő képviselője:	**A polgármester kijelölése alapján Széll Gáborné Blaskó Erzsébet jegyző**
Adatkezelő képviselőjének elérhetősége:	**+36 (36) 492-000; polghiv@szihalom.t-online.hu**

2.3. Az Adatkezelő adatvédelmi tisztviselője:

Az Adatkezelő e szabályzat II. Fejezetének 6. pontja alapján adatvédelmi tisztviselőt vesz igénybe.

Adatvédelmi tisztviselő megnevezése:	**Dr. Pető Balázs**
DPO elérhetőségei:	**info@petobalazs.hu**

2.4. E szabályzat alkalmazhatósága:

Az e szabályzatban foglalt rendelkezéseket az Adatkezelő, mint szervezet többi szabályzatának előírásaival összhangban kell értelmezni. Amennyiben a személyes adatok védelmével kapcsolatosan ellentmondás áll fenn jelen rendelkezések és bármely más, jelen szabályzat hatálybalépése előtt hatályba lépett szabályzat előírásai között, úgy jelen rendelkezések az irányadóak.

3. JOGSZABÁLYI KÖRNYEZET:

A szabályzatban a következő jogszabályi rövidítéseket alkalmazzuk:

GDPR	az Európa 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
Infotv.	Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény
Kjt.	a közalkalmazottak jogállásáról szóló 1992. évi XXXIII. törvény
Ptk.	a Polgári Törvénykönyvről szóló 2013. évi V. törvény

4. ÉRTELMEZŐ RENDELKEZÉSEK

A jelen szabályzat fogalmi rendszere megegyezik a GDPR-ben meghatározott értelmező fogalommagyarázatokkal.

- ***Érintett:*** bármely meghatározott, személyes adat alapján azonosított vagy - közvetlenül vagy közvetve - azonosítható természetes személy;
- ***Személyes adat:*** az érintettel kapcsolatba hozható adat - különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret -, valamint az adatból levonható, az érintettre vonatkozó következtetés;
- ***Különleges adat:***
    - a faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviseleti szervezeti tagságra, a szexuális életre vonatkozó személyes adat,
    - az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat, valamint a bűnügyi személyes adat;

- ***Bűnügyi személyes adat:*** a büntetőeljárás során vagy azt megelőzően a bűncselekménnyel vagy a büntetőeljárással összefüggésben, a büntetőeljárás lefolytatására, illetve a bűncselekmények felderítésére jogosult szerveknél, továbbá a büntetés-végrehajtás szervezeténél keletkezett, az érintettel kapcsolatba hozható, valamint a büntetett előéletre vonatkozó személyes adat;

- ***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;

- ***Tiltakozás:*** az érintett nyilatkozata, amellyel személyes adatának kezelését kifogásolja, és az adatkezelés megszüntetését, illetve a kezelt adat törlését kéri;

- ***Adatkezelő:*** az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely önállóan vagy másokkal együtt az adat kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja;

- ***Adatkezelés:*** az alkalmazott eljárástól függetlenül az adaton végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adat további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése;

- ***Adattovábbítás:*** az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele;

- ***Nyilvánosságra hozatal:*** az adat bárki számára történő hozzáférhetővé tétele;

- ***Adattörlés:*** az adat felismerhetetlenné tétele oly módon, hogy a helyreállítása többé nem lehetséges;

- ***Adatzárolás:*** az adat azonosító jelzéssel ellátása további kezelésének végleges vagy meghatározott időre történő korlátozása céljából;

- ***Adatmegjelölés:*** az adat azonosító jelzéssel ellátása annak megkülönböztetése céljából;

- ***Adatmegsemmisítés:*** az adatot tartalmazó adathordozó teljes fizikai megsemmisítése;

- ***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;

- ***Adatfeldolgozó:*** az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely szerződés alapján - beleértve a jogszabály rendelkezése alapján kötött szerződést is - adatok feldolgozását végzi;

- ***Adatállomány:*** az egy nyilvántartásban kezelt adatok összessége;

- ***Harmadik személy:*** olyan természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely nem azonos az érintettel, az adatkezelővel vagy az adatfeldolgozóval;

- ***EGT-állam:*** az Európai Unió tagállama és az Európai Gazdasági Térségről szóló megállapodásban részes más állam, továbbá az az állam, amelynek állampolgára az Európai Unió és tagállamai, valamint az Európai Gazdasági Térségről szóló megállapodásban nem részes állam között létrejött nemzetközi

szerződés alapján az Európai Gazdasági Térségről szóló megállapodásban részes állam állampolgárával azonos jogállást élvez;

- ***Harmadik ország:*** minden olyan állam, amely nem EGT-állam;

- ***Adatvédelmi incidens:*** személyes adat jogellenes kezelése vagy feldolgozása, így különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés.

- ***Adatkezelés korlátozása:*** a tárolt személyes adatok megjelölése jövőbeli kezelésük korlátozása céljából;

- ***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

- ***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;

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

- ***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;

- ***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;

- ***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;

- ***Képviselő:*** az az Unióban tevékenységi hellyel, illetve lakóhellyel rendelkező és az adatkezelő vagy adatfeldolgozó által 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;

- ***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;

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

- ***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;

- ***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;

- ***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;

- ***Vállalkozás:*** gazdasági tevékenységet folytató természetes vagy jogi személy, függetlenül a jogi formájától, ideértve a rendszeres gazdasági tevékenységet folytató személyegyesítő Társaságokat és egyesületeket is;

- ***Vállalkozáscsoport***: az ellenőrző vállalkozás és az általa ellenőrzött vállalkozások;

Amennyiben a hatályos adatvédelmi jogszabály fogalommagyarázatai eltérnek jelen szabályzat fogalommagyarázataitól, akkor a hatályos jogszabály által meghatározott fogalmak az irányadóak.

II. ÁLTALÁNOS RENDELKEZÉSEK

5. AZ ADATKEZELÉSI ALAPELVEK ÉS ÉRVÉNYESÜLÉSÜK

Az információs önrendelkezés joga alkotmányos – Magyarország Alaptörvényében rögzített – alapjog.

A személyes adat kezelése során be kell tartani a GDPR-ben rögzített, következőkben kifejtett alapelveket.

5.1. Jogszerűség, tisztességes eljárás és átláthatóság:

A személyes adatok kezelését jogszerűen és tisztességesen, az érintett számára átlátható módon kell végezni. A személyes adatok kezelésekor a természetes személyek számára átláthatóvá kell tenni a rájuk vonatkozó személyes adataik gyűjtésének és felhasználásának módját, miként jét, az adatok kezelésének mértékét, továbbá az azokba való betekintés lehetőségét és módját. **Az átláthatóság elve megköveteli, hogy a személyes adatok kezelésével összefüggő tájékoztatás, illetve kommunikáció könnyen hozzáférhető és közérthető legyen, valamint hogy azt világosan és egyszerű nyelvezettel fogalmazzák meg.** Annak biztosítása érdekében, hogy a személyes adatok kezelése az érintett számára átlátható legyen, az **Adatkezelő minden adatkezelésről adatkezelési tájékozatót készít, amelyet az érinttettek számára nyilvánosan és korlátozásmentesen hozzáférhetővé tesz.**

Az adatkezelési tájékozatók megfelelőségét felül kell vizsgálni:

a) a bevezetést követő évtől kezdődően évente legalább egyszer, minden év december 31. napjáig, valamint
b) a GDPR módosítása, továbbá
c) az adatkezelési tevékenységre vonatkozó ágazati jogszabály jelentősebb változása

esetén.

Az adatkezelési tájékoztató lehet:

a) általános vagy
b) egyedi.

A nyilvános és korlátozásmentes hozzáférést szervezetünknél az alábbiak szerint biztosítjuk: Adatkezelési szabályzatunkat és az adatkezelési tájékoztatók közül az általános-, valamint a honlapon történő adatkezeléssel összefüggő egyedi tájékoztatóinkat közzétesszük az önkormányzat hivatalos honlapján (www.szihalom.hu). Azon egyedi tájékoztatóinkat, amelyek olyan eljárásokhoz kapcsolódnak, amelyeket az érintettek online is meg tudnak indítani, szintén honlapunkon tesszük közzé.

A szabályzat, illetve valamennyi tájékoztató megtalálható az önkormányzat székhelyén a polgármesteri titkárságunkon, illetve az ügyben eljárni jogosult munkatársunknál is.

Amennyiben mi kezdeményezünk valamilyen tevékenységet az érintett irányába, úgy az első kapcsolatfelvételkor a tevékenységre irányadó egyedi-, valamint az általános adatvédelmi tájékoztatót átadjuk vagy megküldjük az érintett részére.

5.2. Célhoz kötöttség:

A személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történhet. A személyes adatok nem kezelhetők ezekkel a célokkal össze nem egyeztethető módon. Annak biztosítása érdekében, hogy a személyes adatok kezelése csak az adott célhoz kötött legyen, **az Adatkezelőnek már az adatkezelési tevékenység megkezdését megelőzően meg kell számba kell vennie, hogy az adatkezeléssel mit kíván elérni, mi a tevékenység célja, a cél legitim-e, továbbá a cél eléréséhez mely szemmélyes adatok kezelése szükséges.** Adatkezelő az általa kezelt adatok célhoz kötöttségét bevezetést követő évtől kezdődően évente legalább egyszer, minden év december 31. napjáig felülvizsgálja és ennek megfelelően az adatokat módosítja, törli.

5.3. Adattakarékosság:

A személyes adatoknak az adatkezelés céljai szempontjából megfelelőnek és relevánsnak kell lenniük, valamint csak a szükségesre szabad korlátozódniuk. Annak biztosítása érdekében, hogy a személyes adatok kezelése csak a szükséges mértékű legyen, Adatkezelő az általa kezelt adatokat, **azok relevanciáját** bevezetést követő évtől kezdődően évente legalább egyszer, minden év december 31. napjáig felülvizsgálja és ennek megfelelően az adatokat módosítja, töröli.

5.4. Pontosság:

A személyes adatoknak, pontosnak és szükség esetén naprakésznek kell lenniük, azaz minden ésszerű intézkedést meg kell tenni annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul töröljék vagy helyesbítsék. Annak biztosítása érdekében, hogy a személyes adatok megfelelő pontosságúak legyenek, a szervezeti egységek az általuk kezelt adatokat, azok pontosságát, megfelelőségét bevezetést követő évtől kezdődően évente legalább egyszer, minden év december 31. napjáig felülvizsgálja és ennek megfelelően az adatokat módosítja, törli.

5.5. Korlátozott tárolhatóság:

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 kezelése ezt követően is igazolhatóan szükséges.

Annak biztosítása érdekében, hogy a személyes adatok tárolása a szükséges időtartamra korlátozódjon, a **Adatkezelő** minden adatkezelése tekintetében **adattörlési határidőt** állapít meg az iratkezelési szabályzatában vagy más egyedi intézkedésében, ezt a határidőt pedig **az adatkezelési nyilvántartásában felvezeti.**

Az adattörlési határidők megfelelőségét felül kell vizsgálni:

a) évente legalább egyszer, bevezetést követő évtől kezdődően minden év december 31. napjáig,
b) Az Infotv. vagy a GDPR módosítása esetén, továbbá
c) az iratkezelésre irányadó releváns jogszabályok jelentősebb változásai

esetén.

5.6. Integritás és bizalmas jelleg:

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.

Az integritás és bizalmas jelleg alapelvének érvényesülésre jutását szolgálják az adatszivárgás megelőzésére tett **szervezési, technikai intézkedések**, amelyeket incidens bekövetkezése esetén haladéktalanul, továbbá az incidens bekövetkezésétől függetlenül is a bevezetést követő évtől kezdődően évente legalább egyszer, december 31. napjáig felül kell vizsgálni.

A szervezetnél az adatkezelést végző alkalmazottak és a szervezet megbízásából az adatkezelésben résztvevő, annak valamely műveletét végző szervezetek alkalmazottjai kötelesek a megismert személyes adatokat üzleti titokként megőrizni. **A személyes adatokat kezelő és azokhoz hozzáférési lehetőséggel rendelkező személyek kötelesek titoktartási nyilatkozatot tenni** (1. függelék).

5.7. Elszámoltathatóság:

Az elszámoltathatóság elvének értelmében **az adatkezelő felelős a fenti alapelveknek való megfelelésért, továbbá képesnek kell lennie e megfelelés igazolására.**

Adatkezelő ennek érdekében az adatkezeléssel kapcsolatos valamennyi iratát zárt rendszerben iktatja, helyreállítható formátumban. Az egyes adatkezeléssel kapcsolatos iratokat Adatkezelő erre kijelölt munkatársai őrzik papír alapú és/vagy elektronikus dokumentumban.

6. AZ ADATKEZELŐ ADATVÉDELMI RENDSZERE

Az Adatkezelő szervezeti sajátosságaiból fakadóan (közfeladatot ellátó szervezet) köteles:

a) **e szabályzat megalkotására és jóváhagyására, valamint**
b) **adatvédelmi tisztviselő megbízására.**

Az adatvédelem szervezete – tekintettel a fentiekre is – a következők szerint kerül meghatározásra:

6.1. Az Adatkezelő, mint szervezet vezetője, a szervezet egyéb vezetői

Az Adatkezelő mindenkori **vezetője** (a polgármester) a **jegyző közreműködésével**, az Adatkezelő sajátosságainak figyelembe vételével meghatározza az adatvédelem szervezetét, az adatvédelemre, valamint az azzal összefüggő tevékenységre vonatkozó feladat- és hatásköröket.

A vezető az adatvédelemmel kapcsolatosan:

a) **felelős az érintettek**nek GDPR-ben meghatározott **jogainak gyakorlásához szükséges feltételek biztosításáért;**

b) felelős az Adatkezelő által kezelt személyes adatok védelméhez szükséges **személyi, tárgyi és technikai feltételek biztosításáért;**

c) **felelős** az adatkezelésre irányuló ellenőrzés során esetlegesen **feltárt hiányosságok vagy jogszabálysértő körülmények megszüntetéséért, a személyi felelősség megállapításához szükséges eljárás kezdeményezéséért, illetve lefolytatásáért;**

d) felügyeli az adatvédelmi tisztviselő tevékenységét;

e) **vizsgálatot rendelhet el;**

f) **kiadja az Adatkezelő adatvédelemmel kapcsolatos belső szabályait.**

A szabályzatban előírtak betartatásáért alapvetően a szervezet vezetője a felelős.

A szervezetet harmadik felek irányába a jegyző képviseli.

6.2. Az adatkezelő egyéb munkatársai

Az Adatkezelő **munkatársai** munkájuk során gondoskodnak arról, hogy jogosulatlan személyek ne tekinthessenek be személyes adatokba, továbbá arról, hogy a személyes adat tárolása, elhelyezése úgy kerüljön kialakításra, hogy az jogosulatlan személy részére ne legyen hozzáférhető, megismerhető, megváltoztatható, megsemmisíthető.

Az adatvédelmi tisztviselővel való kapcsolattartásra, továbbá az adatvédelmi alapdokumentumok elkészítésében való közreműködésre Adatkezelő a Szihalmi Közös Önkormányzati Hivatal gazdasági vezetői feladatokat ellátó munkatársát jelöli ki (**adatvédelmi kapcsolattartó**).

6.3. Az adatvédelmi tisztviselő

6.3.1. Az adatvédelmi tisztviselő adatvédelemmel kapcsolatos feladatai:

a) **tájékoztat és szakmai tanácsot ad** az adatkezelő vagy az adatfeldolgozó, továbbá az adatkezelést végző alkalmazottak részére az Rendelet, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezések szerinti kötelezettségeikkel kapcsolatban;
b) **ellenőrzi** a GDPR-nek, 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 vevő személyzet tudatosság-növelését és képzését, valamint a kapcsolódó auditokat is;
c) **kérésre szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan**, valamint nyomon követi a hatásvizsgálat 35. cikk szerinti elvégzését;

d) **együttműködik a felügyeleti hatósággal**;

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

Az adatvédelmi tisztviselő feladatait az adatkezelési műveletekhez fűződő kockázat megfelelő figyelembevételével, az adatkezelés jellegére, hatókörére, körülményére és céljára is tekintettel végzi.

6.3.2. Az adatvédelmi tisztviselő jogállása:

Az adatvédelmi tisztviselőt **szakmai rátermettség, az adatvédelmi jog és gyakorlat szakértői szintű ismerete alapján kell kijelölni.**

Adatkezelő az **adatvédelmi tisztviselő nevét és elérhetőségét bejelenti a NAIH részére.**

Adatkezelő biztosítja az adatvédelmi tisztviselő részére a feladat ellátásához szükséges forrásokat, valamint biztosítja számára, hogy a feladatai ellátása során utasításokat senkitől ne fogadjon el, e feladatai ellátásával összefüggésben nem bocsátható el és szankcióval nem sújtható. **Az adatvédelmi tisztviselő szervezetileg közvetlenül az Adatkezelő szervezet vezetőjének tartozik felelősséggel.**

6.4. Az informatikus (rendszergazda) adatvédelemmel kapcsolatos feladatai:

A szervezet kinevezett informatikussal nem rendelkezik, így **az Adatkezelőnél felmerülő informatikai feladatokat a fenntartó önkormányzat önkormányzati hivatala által foglalkoztatott informatikus, mint rendszergazda látja el.**

Az informatikus:

a) ellátja a vonatkozó szerződésben meghatározott rendszergazdai feladatokat;

b) **a szervezet vagy írásos kérelme alapján közreműködik az adatkezelők egyéni kódjának, jelszavának, jogosultságának beállításában** azon szerverek tekintetében, amelyekre adminisztrátori jogosultsággal rendelkezik;

c) használatba állítás előtt ellátja a szoftverek és hardverek rendszerbe állítását (installálását);

d) a szervereken tárolt adatok vonatkozásában gondoskodik a kezelt adatok jogosultak általi hozzáféréséről, módosításáról, illetőleg gondoskodik a tárolt adatok megsemmisülésének megakadályozásáról;

e) igény esetén közreműködik a számítógépen/szerveren tárolt adatok esetében a megadott szempontú adatszolgáltatásban;

f) **elvégzi a szervereken tárolt adatok biztonsági mentését, naplózását;**

g) **vírusfertőzöttség esetén elvégzi a fertőzött informatikai eszköz vírusmentesítését;**

h) szükség szerint ellátja a számítógépek és a hálózat karbantartását, gondoskodik a szerverek üzemszerű működéséről;

i) ellátja az informatikai eszközök szervizelésével kapcsolatos feladatokat, amennyiben megoldható szakszerviz segítsége nélkül;

j) üzemzavar esetén elvégzi az informatikai rendszerek újraindítását, a hálózat alkalmazásainak és adatainak a visszatöltését;

k) folyamatosan üzemelteti a számítógépes hálózatot;

l) **igény esetén segítséget nyújt az adatkezelőknek a számítástechnikai alkalmazások használatánál és az adatbázisok kezelésénél.**

7. AZ ADATKEZELÉS JOGSZERŰSÉGE

A GDPR 6. cikkének (1) bekezdése értelmében **a személyes adatok kezelése kizárólag akkor és annyiban jogszerű, 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.

Az f) pont nem alkalmazható a közhatalmi szervek által feladataik ellátása során végzett adatkezelésre.

A személyes adatok kezelésének jogalapjait a nemzeti jogszabályok tovább konkretizálhatják, ezekre tekintettel kell lenni az adatvédelmi dokumentáció kialakítása során.

Tekintettel arra, hogy Adatkezelő közfeladatot ellátó szerv, a NAIH 2018. évi beszámolója alapján kizárólag a GDPR 6. cikk (1) bekezdésének e) pontja szerinti jogalapot alkalmazhatja, amely magába olvasztja a többi jogalapot.

III. ADATBIZTONSÁGI SZABÁLYOK

8. Az e szabályzatban foglalt előírások és más szabályzatok kapcsolata

Amennyiben Adatkezelő rendelkezik információbiztonsági szabályzattal és az abban foglaltak az e fejezetben foglaltaknál szigorúbb rendelkezéseket állapítanak meg, úgy az információbiztonsági szabályzat rendelkezései az irányadóak. Amennyiben egyéb szabályzat tartalmaz adatbiztonsági rendelkezést úgy az csak abban az esetben alkalmazható, ha az érintett rendelkezés nem ellentétes a lentebb megfogalmazott szabályokkal, egyben azoknál szigorúbb előírást fogalmaz meg.

8.1. ADATBIZTONSÁG

Az adatkezelő és az adatfeldolgozó a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatókörei, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja, ideértve – többek között – adott esetben:

a) a személyes adatok **álnevesítését és titkosítását,**
b) a **személyes adatok kezelésére használt rendszerek folyamatos bizalmas jellegének biztosítását, integritását, rendelkezésre állását és ellenálló képességét,**
c) fizikai vagy műszaki incidens esetén az arra való **képességet,** hogy **a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását kellő időben vissza lehessen álltani,**
d) az adatkezelés biztonságának garantálására hozott technikai és szervezési intézkedéseknek **hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárást.**

8.2. AZ INFORMÁCIÓBIZTONSÁGI KONTROLLOK TÍPUSAI

Az információbiztonság célrendszeréből kiindulva [bizalmasság (confidentiality), sérthetetlenség (integrity), rendelkezésre állás (availability); röviden: CIA-elv] kiindulva három típusú kontrollt különböztethetünk meg:

a) fizikai kontrollok
b) logikai kontrollok, valamint
c) adminisztratív kontrollok.

8.2.1. Fizikai kontroll

A fizikai kontroll **az iratokhoz és a számítógépes környezethez való hozzáférés korlátozása,** valamint **a rendszeres adatmentés** biztosítását foglalja magában.

Szervezetünknél az alábbi fizikai kontrollok kerültek bevezetésre:

a) Az Adatkezelő székhelye riasztóval rendelkezik. A riasztókhoz tartozó kódokat kizárólag munkatársaink ismerik.
b) Az Adatkezelő által használt helyiségekben zárható szekrények kerülnek alkalmazásra.
c) Az Adatkezelő fő tevékenységi helyén zárhatók az irodák.

d) Az Adatkezelő valamennyi jelszavakat alkalmaz minden munkaállomás esetén, ideértve a hibernálás/képernyőkímélő kötelező alkalmazását, amelyet csak jelszóval lehet kikapcsolni.
e) A jelszavakat jelszó-házirend alapján kell képezni, gondoskodni kell arról, hogy azok legalább hathavonként megváltoztatásra kerüljenek.
f) Be kell tartani a „tiszta asztal" elvét, azaz gondoskodni kell arról, hogy amennyiben a munkatárs munkavégzésének helyét a nap végén vagy nap közben akár csak ideiglenes jelleggel elhagyja, úgy minden, személyes adatot akár csak potenciálisan tartalmazható dokumentuma zárható szekrénybe vagy zárható fiókba kerüljön.

Amennyiben a papíralapon tárolt személyes adat kezelésének célja megvalósult, úgy az Adatkezelő intézkedik a papír megsemmisítéséről.

A megsemmisítés során Adatkezelő iratkezelési szabályzata alapján kell eljárni.

Amennyiben a személyes adatok adathordozója nem papír, hanem más fizikai eszköz, úgy a fizikai eszköz megsemmisítésére a papíralapú dokumentumokra vonatkozó megsemmisítési szabályok az irányadóak.

A számítógépen, illetve hálózaton tárolt személyes adatok biztonsága érdekében Adatkezelő az alábbi intézkedéseket és garanciális elemeket alkalmazza:

a) **az adatkezelés során használt számítógépek az Adatkezelő tulajdonát képezik**, vagy azok fölött tulajdonosi jogkörrel megegyező joggal bír az Adatkezelő;

b) **az adatokkal történő minden számítógépes rekord nyomon követhetően naplózásra kerül**;

c) amennyiben **az adatkezelés célja megvalósult**, az adatkezelés határideje letelt, úgy az **adatot tartalmazó fájl visszaállíthatatlanul törlésre kerül, az adat újra vissza nem nyerhető;**

d) a **hálózaton tárolt adatok biztonsága érdekében a szerveren folyamatos tükrözéssel kerüli el az Adatkezelő az adatvesztést;**

e) **a személyes adatokat tartalmazó adatbázisok aktív adataiból napi mentést végez**, a mentés a központi szerver teljes adatállományára vonatkozik és mágneses adathordozóra történik;

f) a lementett adatokat tároló mágneses adathordozó az erre a célra kialakított páncéldobozban tűzbiztos helyen és módon kerül tárolásra;

g) a személyes adatokat kezelő hálózaton a vírusvédelemről folyamatosan gondoskodik;

h) a rendelkezésre álló számítástechnikai eszközökkel, azok alkalmazásával megakadályozza illetéktelen személyek hálózati hozzáférését.

8.2.2. Logikai kontroll

Szervezetünknél az alábbi logikai kontrollok kerültek bevezetésre:

a) Jelszó-házirend
b) Jogosultságkezelés rendje

A jogosultságkezelés szabályozásának célja, hogy a kiosztott jogosultságok pontosan nyomon követhetőek legyenek, dokumentált formában megőrzésre kerüljenek, valamint az egyes jogosultságokkal rendelkező

személyek tevékenysége és az általuk felhasznált adatok köre ellenőrizhető legyen. Ezen adatok naprakészsége nagymértékben hozzásegíti Adatkezelőt a tőle elvárt, illetve általa elérhető biztonsági szint teljesítéséhez, továbbá az informatikai hálózat törvényi és szakmai normák szerinti üzemeltetéséhez.

Az informatikai rendszerben a jogosultságok változásait (létező jogosultságok, új jogosultságok kiosztása, módosítása, megszűnése) dokumentálni kell.

A személyes adatok biztonsága érdekében Adatkezelő az alábbi jogosultságkezelési előírásokat alkalmazza:

a) **Új jogosultság beállítását**, illetve jogosultság megváltoztatását a jogosultság birtokosának felhatalmazása alapján a **rendszergazda végzi**.

b) A jogosultságok megállapítása során **kizárólag a munkavégzéshez szükséges és elégséges jogosultságokat kell kiosztani**.

c) **El kell kerülni, hogy teljes hozzáférést, illetve adminisztrátori jogosultságokat kapjanak más munkát végző,** illetve a jogosultság birtoklására nem igényt tartó **személyek**.

d) **Adminisztrátori jogosultsággal rendelkező nevesített felhasználót kell alkalmazni a rendszer adminisztrálása érdekében minden esetben, ahol ez lehetséges.** A nem nevesített rendszergazdai jelszavakat zárt borítékban, felbontást gátló módon, aláírva kell tárolni. Ezek használatát az adatkezelő vezető tisztségviselője vagy akadályoztatása esetén helyettesítési rend szerinti helyettese engedélyezheti. A nem nevesített felhasználói jogosultságok használatát indokolni és dokumentálni kell.

e) **Külső – karbantartó vagy fejlesztő – cég alkalmazottja folyamatosan működő, korlátlan időre szóló hozzáférési jogosultsággal nem rendelkezhet**.

Jogosultságkezelési folyamat

Jogosultság igényléséhez vagy módosításához az e szabályzat függeléke szerinti igénylőlapot kell kitölteni. Az igénylőlapot **a jegyzővel kell írásban jóváhagyatni**, majd továbbítani kell a rendszergazda részére.

A jóváhagyást követően a rendszergazda beállítja a jogosultságokat, amelyről visszaigazolást küld az igénylő felé.

Amennyiben a jogosultsággal rendelkező **munkatárs jogviszonya megszűnik**, vagy az általa ellátandó feladatkör módosul és ezáltal meglévő, ám a feladatkör ellátásához a továbbiakban már nem szükséges jogosultságokat haladéktalanul törölni kell. Ennek érdekében **a munkáltató a jegyző útján haladéktalanul kezdeményezi a rendszergazdánál a jogosultság törlését.** A törlésről a rendszergazda köteles visszajelzést küldeni.

Áthelyezés esetén a korábbi munkakör feletti munkáltatói jogokat gyakorló felettes és az új munkakör feletti munkáltatói jogokat gyakorló felettes egyetemlegesen kötelesek gondoskodni a régi jogosultságok törlésének, módosításának vagy új jogosultságok felvételének kezdeményezéséről.

Az informatikai rendszerben a kilépő felhasználók profiljait fel kell függeszteni, használaton kívül kell helyezni. **A felhasználói fiókok törlése a rendszerek ellenőrzését követően történhet meg, ha a törlés nem okoz adatvesztést.**

8.2.3. Adminisztratív kontroll

Az adminisztratív kontrollokat a szervezet belső szabályozói, rendelkezései, eljárásrendjei tartalmazzák. Az Adatkezelőnek e körben rendelkeznie szükséges minimálisan egy üzletmenet-folytonossági tervvel, valamint egy katasztrófaelhárítási tervvel.

Az adminisztratív kontrollokat a fentieken túl az alábbi dokumentumok tartalmazzák:

a) Szervezeti és működési szabályzat,
b) Alapító okirat,
c) Iratkezelési szabályzat,
d) Helyiségek használatának szabályzata,
e) Gazdálkodási szabályzat,
f) Pénzkezelési szabályzat,
g) Vagyonvédelmi szabályzat,
h) Kulcsátvételi nyilatkozatok,
i) Ügyiratkezelési szabályzat,
j) Munkavédelmi szabályzat,
k) tűzvédelmi szabályzat.

Az adminisztratív védelem biztosítása érdekében szervezetünk rendszeresen, de legalább évi egy alkalommal adatbiztonsági tudatossággal összefüggő képzést tart, amelyen valamennyi, a szervezet által alkalmazott munkatárs köteles részt venni.

A saját eszközön történő munkavégzés (Bring Your Own Device; BYOD) szervezetünknél tilos, csakúgy, mint a szervezet eszközeinek magáncélú használata.

A szervezet által a dolgozó részére biztosított valamennyi eszközön (ide értve a használatra átadott mobil eszközöket is) csak az informatikus rendelkezik adminisztrátori jogosultságokkal, így az alkalmazások telepítése ellenőrzött, a felhasználó által nem lehetséges. Ezen eszközökön tilos a magáncélú fájlok tárolása.

IV. AZ ADATKEZELÉSI TEVÉKENYSÉGEKRE VONATKOZÓ RENDELKEZÉSEK

9. Adatkezelő adatkezelési tevékenységei és az adatkezelési nyilvántartások

Adatkezelő a GDPR 30. cikk (1) bekezdése értelmében köteles az általa végzett adatkezelési tevékenységekről nyilvántartást vezetni.

A nyilvántartás az alábbiakat tartalmazza:

a) **az adatkezelő neve és elérhetősége**, valamint – ha van ilyen – a közös adatkezelőnek, az adatkezelő képviselőjének és az **adatvédelmi tisztviselőnek a neve és elérhetősége**;

b) **az adatkezelés céljai**;

c) az **érintettek kategóriáinak**, valamint **a személyes adatok kategóriáinak ismertetése**;

d) olyan címzettek kategóriái, **akikkel a személyes adatokat közlik** vagy közölni fogják, ideértve a harmadik országbeli címzetteket vagy nemzetközi szervezeteket;

e) adott esetben a személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk, beleértve a harmadik ország vagy a nemzetközi szervezet

azonosítását, valamint a 49. cikk (1) bekezdésének második albekezdése szerinti továbbítás esetében a megfelelő garanciák leírása;

f) ha lehetséges, a különböző **adatkategóriák törlésére előirányzott határidők**;

g) ha lehetséges, a GDPR 32. cikk (1) bekezdésében említett **technikai és szervezési intézkedések általános leírása.**

Adatkezelő adatkezelési tevékenységeinek nyilvántartását e szabályzat 2. melléklete tartalmazza.

10. Adattovábbítás és az adattovábbítások nyilvántartása

10.1. ADATTOVÁBBÍTÁS BELFÖLDÖN

Az Adatkezelő **személyes adatot az érintett önkéntes**, az adatkezelés körülményeit illetően tájékozott **hozzájárulása hiányában csak jogszabály felhatalmazása alapján, a jogszabályban meghatározott szerv vagy személy részére**, és csak jogszabályban meghatározott adatkörben, a célhoz kötöttség elvének maradéktalan érvényesítésével **továbbíthat**.

Az **adattovábbítás tényéről az érintettet** – előzetesen, az adatkezelési tájékoztató megismertetésével, erre irányuló kérése esetén egyedileg is **tájékoztatni kell**. Mindezek érdekében az adatkezelő **adattovábbítási nyilvántartást vezet** vagy az adatkezelési tevékenység vonatkozásában olyan elektronikus naplózást alkalmaz, amelyből a nyilvántartáshoz szükséges adatok utólag is kinyerhetők.

Az adattovábbítási nyilvántartás az alábbiakat tartalmazza:

a) a személyes adatok továbbításának időpontját,
b) a továbbított adatköröket,
c) az adattovábbítás jogalapját,
d) az adattovábbítás címzettjét, valamint
e) az adattovábbításért felelős személy nevét és elérhetőségét.

Amennyiben az **adattovábbítás szervezeten belül** történik, abban az esetben is gondoskodni kell arról, hogy a személyes adat csak olyan személy részére kerüljön továbbításra, aki megfelelő hozzáférési jogosultsággal rendelkezik (összhangban a célhoz kötöttség alapelvével).

Az adatátadás kizárólag **abban az esetben nem minősül adattovábbításnak, ha a személyes adat átadása adatfeldolgozónak történik.** Az adatfeldolgozó kilétéről, a részére továbbított személyes adatok köréről az érintetettet előzetesen tájékoztatni kell.

10.2. ADATTOVÁBBÍTÁS KÜLFÖLDRE VAGY NEMZETKÖZI SZERVEZET SZÁMÁRA

Az EGT-tagállamokba irányuló adattovábbítást úgy kell tekintenünk, mintha Magyarország területén belüli adattovábbításra kerülne sor.

Nem EGT-tagállamba történő adattovábbításra csak a felügyeleti hatóság külön engedélyével kerülhet sor, kivéve, ha a Bizottság megállapította, hogy a harmadik ország, a harmadik ország valamely területe, vagy egy vagy több meghatározott ágazata, vagy a szóban forgó nemzetközi szervezet megfelelő védelmi szintet biztosít. Ez utóbbi adattovábbításokhoz nem szükséges külön engedély.

Amennyiben a Bizottság nem hozott a fentiek szerinti határozatot, úgy az Adatkezelő csak abban az esetben továbbíthat személyes adatokat harmadik országba vagy nemzetközi szervezet részére, ha az adatkezelő vagy adatfeldolgozó megfelelő garanciákat nyújtott és csak azzal a feltétellel, hogy az érintettek számára érvényesíthető jogok és hatékony jogorvoslati lehetőségek állnak rendelkezésre.

A megfelelő garanciákat a GDPR tartalmazza (kötelező erejű vállalati szabványok, a Bizottság által elfogadott általános adatvédelmi kikötések, jóváhagyott magatartási kódex, jóváhagyott tanúsítási mechanizmus, stb.).

Személyes adat harmadik országbelinek minősülő online portálra történő továbbítása (különösen: Facebook, Google) külföldre történő adattovábbításnak számít, így vizsgálni kell a fenti körülmények fennállását.

11. Az adatkezelő szervezet, mint adatfeldolgozó

Adatkezelő egyes esetekben adatfeldolgozóként is eljárhat. **Amennyiben adatfeldolgozóként jár el, úgy nyilvántartást vezet az adatkezelő nevében végzett adatkezelési tevékenységek minden kategóriájáról**; a nyilvántartás a következő információkat tartalmazza:

a) az **adatfeldolgozó** vagy adatfeldolgozók **neve és elérhetőségei**, és **minden olyan adatkezelő neve és elérhetőségei, amelynek vagy akinek a nevében az adatfeldolgozó eljár**, továbbá – ha van ilyen – az adatkezelő vagy az adatfeldolgozó képviselőjének, valamint az adatvédelmi tisztviselőnek a neve és elérhetőségei;

b) **az egyes adatkezelők nevében végzett adatkezelési tevékenységek kategóriái**;

c) adott esetben a személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítása, beleértve a harmadik ország vagy a nemzetközi szervezet azonosítását, valamint a GDPR 49. cikk (1) bekezdésének második albekezdése szerinti továbbítás esetében a megfelelő garanciák leírása;

d) ha lehetséges, a GDPR 32. cikk (1) bekezdésében említett technikai és szervezési intézkedések általános leírása.

Adatkezelő, mint adatfeldolgozó adatkezelési tevékenységeinek nyilvántartását e szabályzat függeléke tartalmazza.

Adatfeldolgozói tevékenységet Adatkezelő csak adatfeldolgozói megállapodás alapján végezhet.

12. Adatfeldolgozók igénybevétele

Adatkezelő működése, illetve egyes feladatai ellátása során adatfeldolgozókat vehet igénybe.

Adatfeldolgozó az, aki az **adatkezelést az Adatkezelő nevében végzi.**

Csak **olyan adatfeldolgozó igénybevétele engedélyezett**, aki vagy amely **megfelelő garanciákat nyújt az adatkezelés a GDPR követelményeinek való megfelelését és az érintettek jogainak védelmét biztosító megfelelő technikai és szervezési intézkedések végrehajtására.**

Az adatfeldolgozó által végzett adatkezelést az uniós jog vagy tagállami jog alapján létrejött **olyan** – az adatkezelés tárgyát, időtartamát, jellegét és célját, a személyes adatok típusát, az érintettek kategóriáit, valamint az adatkezelő kötelezettségeit és jogait meghatározó – **szerződésnek vagy más jogi aktusnak kell szabályoznia, amely köti az adatfeldolgozót az adatkezelővel szemben.** A szerződés vagy más jogi aktus **különösen előírja, hogy az adatfeldolgozó:**

a) **a személyes adatokat kizárólag az adatkezelő írásbeli utasításai alapján kezeli** – beleértve a személyes adatoknak valamely harmadik ország vagy nemzetközi szervezet számára való továbbítását is –, kivéve akkor, ha az adatkezelést az adatfeldolgozóra alkalmazandó uniós vagy tagállami jog írja elő; ebben az esetben erről a jogi előírásról az adatfeldolgozó az adatkezelőt az adatkezelést megelőzően értesíti, kivéve, ha az adatkezelő értesítését az adott jogszabály fontos közérdekből tiltja;

b) **biztosítja azt, hogy a személyes adatok kezelésére feljogosított személyek titoktartási kötelezettséget vállalnak vagy jogszabályon alapuló megfelelő titoktartási kötelezettség alatt állnak**;

c) meghozza a GDPR 32. cikkében („az adatkezelés biztonsága") előírt intézkedéseket;

d) **tiszteletben tartja a további adatfeldolgozó igénybevételére vonatkozóan a GDPR 28. cikk (2) és (4) bekezdésben említett feltételeket** (további adatfeldolgozó csak előzetes hozzájárulással vehető igénybe, a további adatfeldolgozóra is ugyanazokat az adatvédelmi kötelezettségeket kell telepíteni, mint amelyek az Adatkezelő és az adatfeldolgozó közötti szerződésben létrejöttek);

e) az adatkezelés jellegének figyelembevételével **megfelelő technikai és szervezési intézkedésekkel a lehetséges mértékben segíti az adatkezelőt abban**, hogy **teljesíteni tudja kötelezettségét az érintett GDPR. III. fejezetben foglalt jogainak gyakorlásához kapcsolódó kérelmek megválaszolása tekintetében**;

f) **segíti az adatkezelőt a GDPR 32–36. cikk szerinti kötelezettségek (adatkezelés biztonsága, adatvédelmi incidensek bejelentése és az érintettek tájékoztatása, adatvédelmi hatásvizsgálat lefolytatása, előzetes konzultáció) teljesítésében, figyelembe véve az adatkezelés jellegét és az adatfeldolgozó rendelkezésére álló információkat**;

g) **az adatkezelési szolgáltatás nyújtásának befejezését követően az adatkezelő döntése alapján minden személyes adatot töröl vagy visszajuttat az adatkezelőnek, és törli a meglévő másolatokat**, kivéve, ha az uniós vagy a tagállami jog az személyes adatok tárolását írja elő;

h) az **adatkezelő rendelkezésére bocsát minden olyan információt, amely a GDPR 28. cikkben meghatározott kötelezettségek teljesítésének igazolásához szükséges**, továbbá amely lehetővé teszi és elősegíti az adatkezelő által vagy az általa megbízott más ellenőr által végzett auditokat, beleértve a helyszíni vizsgálatokat is.

Az adatfeldolgozói szerződés mintáját e szabályzat függeléke tartalmazza.

Adatkezelő szervezet – gazdasági szervezettel nem rendelkező szervezetként – több adatkezelési tevékenysége során (különösen: munkaügyekkel, költségvetési gazdálkodással és pénzügyekkel összefüggő tevékenységek) megállapodás alapján Szihalom Községi Önkormányzat önkormányzati hivatalát veszi igénybe.

13. Az adatvédelmi incidens

13.1. AZ INCIDENS BEJELENTÉSE:

Az 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.

Adatkezelő azon **dolgozó**ja, aki az Adatkezelő által kezelt/feldolgozott személyes adatokkal kapcsolatban **adatvédelmi incidenst** (különösen: jogosulatlan hozzáférést, megváltoztatást, továbbítást, nyilvánosságra

hozatalt, törlést, megsemmisítést, vagy véletlen megsemmisülést és sérülést) észlel, **köteles azt Adatkezelő vezetőjének és a jegyzőnek bejelenteni.**

A bejelentésnek minimálisan tartalmaznia kell:

a) a bejelentő nevét és elérhetőségét,
b) az incidens tárgyát, valamint
c) azt a tényt, hogy az incidens informatikai rendszert érint-e.

A vezető – a jegyző és adatvédelmi kapcsolattartó útján – a bejelentést követően haladéktalanul **tájékoztatja a felelős adatvédelmi tisztviselőt** az adatvédelmi incidens bekövetkezéséről, megadva a bejelentő nevét, elérhetőségét, a bejelentett adatvédelmi incidens tárgyát, valamint azt, hogy az incidens informatikai rendszert érint-e. Ha a vezető megállapítja, hogy az incidens informatikai rendszert is érint, akkor a tájékoztatást egyidejűleg meg kell küldeni a rendszergazdának.

Amennyiben a szervezet ellenőrzésre jogosult személyek feladataik ellátása során adatvédelmi incidenst észlelnek, közvetlenül értesítik a felelős adatvédelmi tisztviselőt.

Amennyiben az **adatvédelmi tisztviselő** a fentiek szerint tudomást szerez az incidensről, úgy **a bejelentést megvizsgálja, a bejelentőtől szükség szerint további információt kér, amelyet a bejelentő haladéktalanul köteles megadni.**

Az adatszolgáltatásnak tartalmaznia kell:

a) az incidens bekövetkezésének időpontját és helyét,
b) az incidens leírását, körülményeit, hatásait,
c) az incidens során kompromittálódott adatok körét, számosságát,
d) a kompromittálódott adatokkal érintett személyek körét,
e) az incidens elhárítása érdekében tett intézkedések leírását,
f) a kár megelőzése, elhárítása, csökkentése érdekében tett intézkedések leírását.

Amennyiben az adatszolgáltatás alapján az adatvédelmi incidens további vizsgálatot igényel, annak végrehajtására az adatvédelmi tisztviselő felkéri a szerv vezetőjét (informatikai rendszerben bekövetkezett adatvédelmi incidens esetében a rendszergazdát is bevonva), majd szaktanácsadóként működik közre a vizsgálat lefolytatásában.

A vizsgálat megállapításai alapján az adatvédelmi tisztviselő (informatikai rendszerben bekövetkezett adatvédelmi incidens esetében a rendszergazda véleményével együtt) – **javaslatot tesz az adatvédelmi incidens elhárításához szükséges intézkedésekről a vezető részére**

A javaslat alapján a megvalósítandó további intézkedésekről a vezető dönt.

Az adatvédelmi incidens elhárítása érdekében elrendelt egyes intézkedésekről és azok végrehajtásáról a vezető haladéktalanul tájékoztatja az adatvédelmi tisztviselőt.

13.2. Az incidensek nyilvántartása

Az adatvédelmi incidensekről Adatkezelő nyilvántartást vezet.

A nyilvántartásba rögzíteni kell:

a) az érintett személyes adatok körét,
b) az adatvédelmi incidenssel érintettek körét és számát,
c) az adatvédelmi incidens időpontját,
d) az adatvédelmi incidens körülményeit, hatásait, az adatvédelmi incidens elhárítására megtett intézkedéseket,
e) az adatkezelést előíró jogszabályban meghatározott egyéb adatokat.

A nyilvántartásban szereplő adatvédelmi incidensekre vonatkozó adatokat személyes adatokat érintő incidens esetében 5 évig, különleges adatokat érintő incidens esetében 20 évig köteles az Adatkezelő megőrizni.

A nyilvántartás mintáját e szabályzat függeléke tartalmazza.

13.3. Hatósági bejelentés és érintettek tájékoztatása az incidensekről

Az adatvédelmi tisztviselő az adatvédelmi incidenst a bekövetkezését követően haladéktalanul, de legkésőbb a bekövetkezéséről való tudomásszerzéstől számított 72 órán belül bejelenti a NAIH részére, kivéve, ha az incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Ha a bejelentés nem történik meg határidőben, az adatvédelmi tisztviselő köteles ennek okát igazolni a NAIH részére.

A hatósági bejelentés tartalmazza

a) az adatvédelmi incidenssel érintett személyek körét és hozzávetőleges számát,
b) az adatvédelmi incidens jellegét, körülményeit,
c) az adatvédelemért felelős személy nevét és elérhetőségét,
d) az adatvédelmi incidens valószínűsíthető következményeit, valamint
e) az adatvédelmi incidens orvoslására és enyhítésére megtett intézkedéseket.

Ha a vizsgálat eredményeként megállapítást nyert, hogy az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira, szabadságaira nézve és az érintettek tájékoztatása szükséges, az adatvédelmi tisztviselő a szervezet vezetőjének közreműködésével haladéktalanul értesíti az érintetteket.

Nem kell az érintetteket értesíteni:

a) ha az Adatkezelő olyan technikai, szervezési, védelmi intézkedéseket hajtott végre az érintett adatokra vonatkozóan, amelyek megakadályozzák az illetéktelen személyek számára való hozzáférést az adatokhoz vagy megakadályozzák az adatok értelmezhetőségét,
b) ha az adatvédelmi incidens bekövetkezését követően az Adatkezelő olyan intézkedéseket tett, amelyek biztosítják, hogy a feltárt adatkezelési kockázat valószínűsíthetően nem valósul meg,
c) ha a tájékoztatás aránytalan erőfeszítést tenne szükségessé.

Ebben az esetben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, mely tájékoztatás elektronikus úton is megtörténhet.

14. Hatásvizsgálat

A GDPR 24. cikk (1) bekezdése alapján Adatkezelő az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre annak biztosítása és bizonyítása céljából, hogy a személyes adatok kezelése a GDPR-ral összhangban történik. Ezeket az intézkedéseket az Adatkezelő felülvizsgálja és szükség esetén naprakésszé teszi. Ennek keretében **a természetes személyek jogaira és szabadságaira nézve magas kockázattal járó esetekben Adatkezelőnek fel kell mérnie a kockázat valószínűségét és súlyosságát.**

A valószínűség és súlyosság felmérésének alapvető módszere az adatvédelmi hatásvizsgálat, amely magában foglalja az említett kockázat mérséklését, a személyes adatok védelmét, valamint a GDPR-nak való megfelelés bizonyítását célzó tervezett intézkedéseket, garanciákat és mechanizmusokat.

Az eredményes kockázatkezeléshez az alábbiak feltárása szükséges:

a) az adatkezelés jellegének meghatározása;
b) az adatkezelési műveletek szükségességének és arányosságának vizsgálata;
c) annak feltárása, hogy milyen kockázatokkal lehet számolni és azok kezelésére milyen intézkedések szolgálhatnak.

Adatvédelmi hatásvizsgálatot különösen az alábbi esetekben kell elvégezni:

a) amikor a személyes adatkezelés célja a természetes személyekkel kapcsolatos döntés meghozatala, méghozzá a természetes személyek személyes jellemzőinek szisztematikus, kiterjedt és automatizált értékelése alapján (pl.: profilalkotás);
b) a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a természetes személyek egyedi azonosítását célzó genetikai és biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok, mint a személyes adatok különleges kategóriáinak kezelése;
c) a büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó személyes adatok nagy számban történő kezelése; vagy
d) nyilvános helyek nagymértékű, módszeres megfigyelése, különösen abban az esetben, ha azt elektronikus optikai eszközök alkalmazásával hajtják végre;
e) ha az illetékes felügyeleti hatóság úgy ítéli meg, hogy az adatkezelés valószínűsíthetően magas kockázattal jár az érintettek jogaira és szabadságaira nézve, különösen mivel megakadályozza, hogy az érintettek a jogaikat gyakorolják, vagy szolgáltatásokat vegyenek igénybe, illetve szerződést érvényesítsenek, esetleg mindössze azért, mert az említett műveletekre szisztematikusan és nagy számban kerül sor.

A hatásvizsgálatot a 9. mellékletben leírt szempontrendszer figyelembevételével kell elvégezni.

15. Érdekmérlegelés és az érdekmérlegelési teszt

Amennyiben az adatkezelés jogalapját a GDPR 6. cikk (1) bekezdés f) pontja képezi, az adatkezelési folyamat, akkor és annyiban lesz jogszerű, amennyiben 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.

Az adatkezelés jogszerűségének vizsgálatához Adatkezelő elvégez egy érdekmérlegelési tesztet, mely során az adatkezelés céljának szükségességét és az érintettek jogainak és szabadságainak arányos mértékű korlátozását vizsgálja és megfelelően alátámasztja.

Az érdekmérlegelési teszt során Adatkezelő azonosítja jogos érdekét az adatkezeléshez, valamint a súlyozás ellenpontját képező érintetti érdeket és az érintett alapjogot. Az egymással ellentétes jogok és érdekek súlyozásának feltételét mindig az adott eset sajátos körülményeire való tekintettel vizsgálja. Adatkezelő a mérlegelés során figyelembe veszi különösen a kezelt, illetve kezelendő adat természetét és szenzitív jellegét, nyilvánosságának mértékét, az esetlegesen bekövetkező szabálysértés súlyosságát, stb.

Az érdekmérlegelési teszt részeként Adatkezelő a szükségesség és arányosság vizsgálatát is elvégzi amelynek értelmében a személyes adatok védelme alóli kivételeknek és a védelem korlátozásainak a feltétlenül szükséges mérték határain belül kell maradniuk. A kezelhető adatok jellege és mennyisége nem haladhatja meg a jogszerű érdekek érvényesítése céljából szükséges mértéket. Az arányosság vizsgálata a célok és a megválasztott eszközök közötti kapcsolat értékelését foglalja magában. A választott eszközök a szükségesség mértékét nem haladhatják meg, azonban az eszközöknek is alkalmasnak kell lenniük a meghatározott cél elérésére.

A súlyozás elvégzése alapján Adatkezelő megállapítja, hogy kezelhető-e a személyes adat.

A teszt eredményéről az érintettek tájékoztatást kapnak, melyből egyértelműen kiderül, hogy mely jogos érdek alapján és miért tekinthető arányos korlátozásnak az, hogy Adatkezelő az érintett beleegyezése nélkül kezeli a személyes adatot, tehát Adatkezelő adatkezeléséhez fűződő jogos érdeke miért múlja felül az érintett érdekeit, illetve jogait. Adatkezelő tájékoztatja az érintetteket a hozzájárulás hiányára tekintettel alkalmazott adatvédelmi garanciákról és az adatkezelés elleni tiltakozás lehetőségeiről.

Noha a NAIH fentebb említett, 2018-as jelentése értelmében az Adatkezelőnél nem kerülhet sor a GDPR 6. cikk (1) bekezdésének f) pontja szerinti adatkezelésre, minden olyan esetben, amelynél a jelentésben foglaltak hiányában a jogos érdek lenne az alkalmazandó jogalap, el kell végezni az e pont szerinti szükségesség-arányosság tesztet.

V. AZ ÉRINTETTI JOGOK

16. Tájékoztatás

Az érintett Adatkezelőtől tájékoztatást kérhet személyes adatai kezeléséről.

Az érintett a tájékoztatás elősegítése érdekében kérelmezheti a betekintést a személyes adatait tartalmazó iratokba, kivéve ha az irat

a) harmadik személy(ek) adatait is tartalmazza,
b) minősített adatot vagy üzleti titkot tartalmaz, vagy
c) döntés-előkészítéssel kapcsolatos és a benne szereplő harmadik személy(ek) adatainak felismerhetetlenné tétele aránytalan többletköltséggel járna.

A tájékoztatás ingyenes, ha a tájékoztatást kérő a folyó évben azonos területre, szervezeti egységre vonatkozó tájékoztatási kérelmet az adatkezelőhöz még nem nyújtott be. Egyéb esetekben a tájékoztatás megadásával együtt járó költségeket az adatgazda, üzleti titok kapcsán az üzleti titokgazda határozza meg, és az érintett köteles viselni.

A költségtérítés mértékét az Adatkezelő és az érintett közötti szerződés is tartalmazhatja.

A már megfizetett költséget a kérelmezőnek vissza kell téríteni, ha az adatokat jogellenesen kezelték, vagy a tájékoztatás kérése helyesbítéshez vezetett.

A kérelmezőt a lehető legrövidebb időn belül, legfeljebb azonban 30 napon belül közérthető formában kell tájékoztatni.

Az érintett tájékoztatását az Adatkezelő akkor tagadhatja meg:

1) **ha az Adatkezelő törvény, nemzetközi szerződés, vagy Európai Unió kötelező jogi aktusnak rendelkezése alapján személyes adatokat úgy vesz át, hogy az adattovábbító adatkezelő egyidejűleg jelzi a személyes adat kezelésének lehetséges célját, lehetséges időtartamát, lehetséges címzettjeit, az érintett GDPR-ben biztosított jogainak korlátozását vagy a kezelésének egyéb korlátozását (együtt adatkezelési korlátozás), és a Hivatal azokat az adatkezelési korlátozásnak megfelelő terjedelemben és módon kezeli, az érintett jogait az adatkezelési korlátozásnak megfelelően biztosítja,** vagy

2) **ha az érintett GDPR-ban biztosított jogait törvény korlátozza az állam külső és belső biztonsága érdekében, így a honvédelem, a nemzetbiztonság, a bűncselekmények megelőzése vagy üldözése, a büntetés-végrehajtás biztonsága érdekében, az Európai Unió jelentős gazdasági vagy pénzügyi érdekéből, valamint a foglalkozások gyakorlásával összefüggő fegyelmi és etikai vétségek, a munkajogi és munkavédelmi kötelezettségszegések megelőzése és feltárása céljából – beleértve minden esetben az ellenőrzést és a felügyeletet is -, továbbá az érintett vagy mások jogainak védelme érdekében.**

Az Adatkezelő a tájékoztatás megtagadása esetén írásban közli az érintettel, hogy a felvilágosítás megtagadása mely rendelkezése alapján került sor és egyben arról is tájékoztatást ad az érintettnek, hogy a tájékoztatás megtagadása miatt jogorvoslattal a bírósághoz, illetve a Hatósághoz fordulhat.

17. Betekintés

Az érintett kérelmére a szervezet illetékes adatgazdája, üzleti titok kapcsán az üzleti titokgazda tájékoztatást ad az általa kezelt, illetőleg feldolgozott adatairól, azok forrásáról, az adatkezelés céljáról, jogalapjáról, időtartamáról, az adatfeldolgozó nevéről, címéről (székhelyéről) és az adatkezeléssel összefüggő tevékenységéről, az érintett adatát érintő adatvédelmi incidens körülményeiről, hatásairól és az elhárítására megtett intézkedésekről, továbbá arról, hogy kik (név; cím, illetőleg székhely) és milyen jogalap alapján, milyen célból kapják vagy kapták meg az adatokat.

Az adatgazda, üzleti titok kapcsán az üzleti titokgazda a közvetlenül hozzá érkezett tájékoztatás iránti kérelmekre köteles a kérelem hozzá történt megérkezésétől számított legrövidebb idő alatt, legfeljebb azonban 7 napon belül írásban tájékoztatást adni.

18. Az érintett előzetes tájékoztatásának követelménye

Az érintettel az adatkezelés megkezdése előtt az adatkezelést végzőnek közölni kell, hogy az adatkezelés hozzájáruláson alapul (önkéntes) vagy kötelező. Kötelező adatkezelés esetén nem szükséges az érintett hozzájárulásának a beszerzése és nem kell az érintettel adatvédelmi nyilatkozatot aláíratni, mert az adatkezelés jogalapja a törvényi felhatalmazás és nem az érintett hozzájárulása. **Az érintettet ebben az esetben is tájékoztatni kell az adatkezelés jogalapjáról,** tehát arról, hogy melyik jogszabály felhatalmazása alapján történik a személyes adatainak kezelése.

Az adatkezelés megkezdése előtt az adatkezelést végzőnek az érintettet - kérés nélkül is - előzetesen egyértelműen és részletesen tájékoztatni kell az adatai kezelésével kapcsolatos minden tényről, így különösen:

a) az adatkezelés kötelező, vagy hozzájáruláson alapuló voltáról,
b) az adatkezelés céljáról és jogalapjáról (önkéntes vagy jogszabály által kötelező),
c) az adatkezelő személyéről, adatfeldolgozás esetén az adatfeldolgozó kilétéről,
d) az adatkezelés időtartamáról,
e) az adattovábbítás címzettjeiről,
f) az érintett jogairól,
g) jogorvoslati lehetőségeiről: adatvédelmi hatósághoz, bírósághoz fordulás,
h) arról, hogy kik ismerhetik meg az adatokat, valamint
i) a szolgáltatás igénybevételének meghiúsulásának tényéről, ha az érintett az ahhoz szükséges személyes adatokat nem adja meg, illetve nem járul hozzá azok kezeléséhez.

A tájékoztatás alapvetően az általános és egyedi adatkezelési tájékoztató átadásával vagy az érintett részére történő megküldésével valósul meg.

Ha az érintett(ek) személyes tájékoztatása lehetetlen vagy aránytalan költséggel járna, a tájékoztatás az alábbi információk nyilvánosságra hozatalával is megtörténhet:

a) az adatgyűjtés ténye,
b) az érintettek köre,
c) az adatgyűjtés célja,
d) az adatkezelés időtartama,
e) az adatok megismerésére jogosult lehetséges adatkezelők személye,
f) az érintettek adatkezeléssel kapcsolatos jogainak és jogorvoslati lehetőségeinek ismertetése.

Mindezek érdekében az Adatkezelő központi honlapján (fuzeskonyvtar.hu) a valamennyi aloldalról elérhető „Adatvédelem" menüpontban nyilvánosságra hozza minimálisan:

a) **a honlapon megvalósuló adatkezeléssel összefüggő adatkezelési tájékoztatóját,**
b) **általános adatkezelési tájékoztatóját, továbbá**
c) **minden olyan egyedi adatkezelési tájékoztatót, amelyek személyes átadására/megküldésére nincs mód, vagy az aránytalan költséggel járna.**

19. Adathordozhatósághoz való jog

Az érintett jogosult lehet arra is, hogy a rá vonatkozó, általa egy adatkezelő rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja, továbbá jogosult arra, hogy ezeket az adatokat egy másik adatkezelőnek továbbítsa anélkül, hogy ezt akadályozná az az adatkezelő, amelynek a személyes adatokat a rendelkezésére bocsátotta.

20. Jogorvoslati lehetőségek

Ha az érintett természetes személy úgy ítéli meg, hogy a rá vonatkozó személyesadat-kezelés nem felel meg a törvényi követelményeknek, panaszt nyújthat be a felügyeleti hatósághoz, a Nemzeti Adatvédelmi és Információszabadság Hatósághoz (NAIH).

Mind az érintett, mint pedig az, akire nézve a NAIH döntése kötelezést tartalmaz, jogosult arra, hogy a döntéssel szemben bírósági felülvizsgálatot kezdeményezzen. Az érintett a NAIH eljárásától függetlenül is jogosult közvetlenül a bírósághoz fordulni.

VI. EGYES KÜLÖNÖS RENDELKEZÉSEK

21. Másolatok készítése személyazonosításra alkalmas igazolványokról

Adatkezelő feladatai ellátása során nem készíthet fénymásolatot személyazonosításra alkalmas igazolványokról. A hatósági okmányról készített fénymásolat önmagában nem alkalmas a természetes személyek azonosítására, mivel az egyén személyes jelenléte is elengedhetetlen az igazolvány alapján történő személyazonosításhoz. Az arcképes hatósági igazolvány értelemszerűen csak akkor rendelkezik bizonyító erővel, ha annak alapján az Adatkezelő megbizonyosodhat arról, hogy az igazolványon szereplő személy képmása és az igazolványt felmutató személy megegyeznek. Egy hatósági igazolványról készített másolat nem rendelkezik bizonyító erővel arról, hogy hiteles másolata egy érvényes hatósági igazolványnak.

Amennyiben mégis szükséges a fentiek szerinti igazolványról másolat készítése, úgy Adatkezelő – tekintettel a célhoz kötöttség és az adattakarékosság alapelvére – kizárólag „maszkolt" másolatot készíthet (a másolás során csak az igazolvány csak azon részei maradhatnak olvasható állapotban, amely adatokat az érintett egyébként is köteles magáról megadni). A fénymásolat ebben az esetben az adategyeztetés céljából készül. A másolatot Adatkezelő azonnal és visszavonhatatlanul törli vagy megsemmisíti, a maszkolt igazolvány-másolatokon szereplő adatok a Adatkezelő kijelölt munkatársa általi összehasonlítását, de legkésőbb a másolat készültét követő 30 nap elteltével.

VII. ZÁRÓ RENDELKEZÉSEK

E szabályzat 2020. szeptember 01. napján lép hatályba.

Kelt: Szihalom, 2020. szeptember 01.

Bóta József Sándor

polgármester