



Szikszó Város Önkormányzata
3800 Szikszó, Kálvin tér 1.
Tel:(46) 596-450; Fax:(46) 596-211
info@szikszo.hu

HATÁROZAT

15/2020.(V.29.) Szikszó Város Önkormányzat Polgármesteri Határozata

Szikszó Város Önkormányzat Polgármestere a veszélyhelyzet kihirdetéséről szóló 40/2020. (III.11.) számú kormányrendelet, valamint a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény 46.§ (4) bekezdésében foglalt jogköre alapján a Képviselő-testület feladat- és hatáskörében eljárva az alábbiak szerint határoz:

Döntés gyermekjóléti és gyermekvédelmi feladatainak ellátásáról szóló beszámoló elfogadásával kapcsolatban

Szikszó Város Önkormányzat Polgármestere elfogadja a gyermekek védelméről és a gyámügyi igazgatásról szóló 1997. évi XXXI. törvény 96. § (6) bekezdése értelmében a helyi önkormányzatok gyermekjóléti és gyermekvédelmi feladatainak ellátásáról szóló beszámolót a határozat mellékletét képező tartalommal.

A Polgármester elrendeli a beszámoló megküldését a Borsod-Abaúj-Zemplén Megyei Kormányhivatal Hatósági Főosztály Szociális és Gyámügyi Osztálya részére.
(Írásos anyag csatolva a jegyzőkönyvhöz: 2. számú melléklet)

Felelős: polgármester

Határidő: azonnal

Kelt: Szikszó, 2020.05.29.



Beszámoló gyermekjóléti és gyermekvédelmi feladatainak ellátásáról

A gyermekek védelméről és a gyámügyi igazgatásról szóló 1997. évi XXXI. törvény 96. § (6) bekezdése értelmében a helyi önkormányzatoknak a gyermekjóléti és gyermekvédelmi feladatainak ellátásáról átfogó értékelést kell készíteni, amelynek tartalma:

- a település demográfiai mutatói, különös tekintettel a 0-18 éves korosztály adataira,
- a rendszeres gyermekvédelmi kedvezményben részesülők száma, kérelmezőkre vonatkozó általánosítható adatok, elutasítások száma, főbb okai, önkormányzatot terhelő kiadás nagysága, egyéb, a Gyvt.-ben nem szabályozott pénzbeli vagy természetbeni juttatásokra vonatkozó adatok,
- gyermekétkeztetés megoldásának módjai, kedvezményben részesülőkre vonatkozó statisztikai adatok,
- az önkormányzat által biztosított személyes gondoskodást nyújtó ellátások bemutatása,
- gyermekjóléti szolgáltatás biztosításának módja, működésének tapasztalata (alapellátásban részesülők száma, gyermekek veszélyeztetettségének okai, válsághelyzetben levő várandós anyák gondozása, családjából kiemelt gyermek szüleinek gondozása, jelzőrendszer tagjaival való együttműködés tapasztalatai), gyermekek napközbeni ellátásának, gyermekek átmeneti gondozásának biztosítása, ezen ellátások igénybevétele, s az ezzel összefüggő tapasztalatokat,
- a felügyeleti szervek által gyámhatósági, gyermekvédelmi területen végzett szakmai ellenőrzések tapasztalatainak, továbbá a gyermekjóléti és gyermekvédelmi szolgáltató tevékenységet végzők ellenőrzésének alkalmával tett megállapítások bemutatását,
- jövőre vonatkozó javaslatok, célok meghatározása a Gyvt. előírásai alapján (milyen ellátásokra és intézményekre lenne szükség a problémák hatékonyabb kezelése érdekében, gyermekvédelmi prevenciók elképzelések),
- a bűnmegelőzési program főbb pontjainak bemutatása (amennyiben a településen készült ilyen program), valamint a gyermekkorú és a fiatalok bűnelkövetők számának az általuk elkövetett bűncselekmények számának, a bűnelkövetés okainak bemutatása,
- a települési önkormányzat és a civil szervezetek közötti együttműködés keretében milyen feladatok, szolgáltatások ellátásában vesznek részt civil szervezetek (alapellátás, szakellátás, szabadidős programok, drogvédelem stb.).

1. A település demográfiai mutatói, különös tekintettel a 0-18 éves korosztály adataira

Szikszó város állandó lakosainak száma 5590 fő.

A gyermekek korcsoportonkénti megoszlása a következőképpen alakult a 2019-es évben:

életkor:	0-2 éves	3-5 éves	6-13 éves	14-18 éves
gyermek	36	33	121	64

2. A rendszeres gyermekvédelmi kedvezményben részesülők száma, kérelmezőkre vonatkozó általánosítható adatok, elutasítások száma, főbb okai, önkormányzatot terhelő kiadás nagysága, egyéb, a Gyvt.-ben nem szabályozott pénzbeli vagy természetbeni juttatásokra vonatkozó adatok

A rendszeres gyermekvédelmi kedvezményre való jogosultság megállapításának célja annak igazolása, hogy a gyermek szociális helyzete alapján jogosult

- az ingyenes vagy kedvezményes intézményi gyermekétkeztetésre és a szünidei gyermekétkeztetésre
- pénzbeli támogatásra (évente két alkalommal)
- törvényben és más jogszabályban meghatározott egyéb kedvezményeknek az igénybevételére.

A rendszeres gyermekvédelmi kedvezményre való jogosultság megállapítását a szülő vagy más törvényes képviselő kérheti, amennyiben a gyermeket gondozó családban az egy főre jutó havi jövedelem összege nem haladja meg

- *a)* az öregségi nyugdíj mindenkori legkisebb összegének (továbbiakban: az öregségi nyugdíj legkisebb összege) a 145%-át, ha
- *aa)* a gyermeket egyedülálló szülő vagy más törvényes képviselő gondozza,
- *ab)* a gyermek tartósan beteg, illetve súlyosan fogyatékos, vagy
- *ac)* a nagykorúvá vált gyermek megfelel a 20. § (2) bekezdésében foglalt feltételeknek;
- *b)* az öregségi nyugdíj legkisebb összegének 135%-át az *a)* pont alá nem tartozó esetben,
- feltéve, hogy a vagyoni helyzet vizsgálata során az egy főre jutó vagyon értéke nem haladja meg külön-külön vagy együttesen a jogszabályban meghatározott értéket.

A települési önkormányzat jegyzője annak a gyermeknek, fiatal felnőttnek, akinek rendszeres gyermekvédelmi kedvezményre való jogosultsága

- *a)* a tárgyév augusztus 1-jén fennáll, a tárgyév augusztus hónapjára tekintettel,

- b) a tárgyév november 1-jén fennáll, a tárgyév november hónapjára tekintettel
- alapösszegű pénzbeli támogatást nyújt, amennyiben gyámhatóság határozata alapján hátrányos vagy halmozottan hátrányos helyzetűnek minősül emelt összegű pénzbeli támogatásra jogosult.

Rendszeres gyermekvédelmi kedvezménnyel kapcsolatos intézkedések

Feladat megnevezése	Gyermekek száma
Rendszeres gyermekvédelmi kedvezményre jogosultak száma	273 fő
Rendszeres gyermekvédelmi kedvezmény iránti kérelem elutasítása	1 fő
Rendszeres gyermekvédelmi kedvezmény megszüntetése	6 fő

Az elutasítás oka a törvény által meghatározott egy főre jutó jövedelem túllépése volt.

A gyermekvédelmi törvény értelmében a hátrányos, halmozottan hátrányos helyzet szempontjából meghatározó tényezők a következők:

A gyermekek védelméről és a gyámügyi igazgatásról szóló 1997. évi XXXI. tv. (továbbiakban Gyvt.) 67/A. § (1) bekezdésében foglaltak alapján **hátrányos helyzetű** az a rendszeres gyermekvédelmi kedvezményre jogosult gyermek és nagykorúvá vált gyermek, aki esetében az alábbi körülmények közül egy fennáll:

- a) a szülő vagy a családbafogadó gyám **alacsony iskolai végzettsége**, ha a gyermeket együtt nevelő mindkét szülőről, a gyermeket egyedül nevelő szülőről vagy a családbafogadó gyámról – önkéntes nyilatkozata alapján – megállapítható, hogy a rendszeres gyermekvédelmi kedvezmény igénylésekor legfeljebb alapfokú iskolai végzettséggel rendelkezik,
- b) a szülő vagy a családbafogadó gyám **alacsony foglalkoztatottsága**, ha a gyermeket nevelő szülők bármelyikéről vagy a családbafogadó gyámról megállapítható, hogy a rendszeres gyermekvédelmi kedvezmény igénylésekor az Szt. 33. §-a szerinti aktív korúak ellátására jogosult vagy a rendszeres gyermekvédelmi kedvezmény igénylésének időpontját megelőző 16 hónapon belül legalább 12 hónapig álláskeresőként nyilvántartott személy,
- c) **a gyermek elégtelen lakókörnyezete, illetve lakáskörülményei**, ha megállapítható, hogy a gyermek a településre vonatkozó integrált városfejlesztési stratégiában szegregátumnak nyilvántartott lakókörnyezetben vagy félkomfortos, komfort nélküli vagy szükséglakásban, illetve olyan lakáskörülmények között él, ahol korlátozottan biztosítottak az egészséges fejlődéshez szükséges feltételek.

Halmozottan hátrányos helyzetű az a rendszeres gyermekvédelmi kedvezményre jogosult gyermek és nagykorúvá vált gyermek, akinek esetében a fenti körülmények közül legalább kettő fennáll, a nevelésbe vett gyermek, az útgondozói ellátásban részesülő és tanulói vagy hallgatói jogviszonyban álló fiatal felnőtt.

A 2019-es évben a hátrányos helyzet megállapítása iránt 96 fő nyújtott be kérelmet. A halmozottan hátrányos helyzetű megállapítása iránt 117 fő nyújtott be kérelmet. A hátrányos illetve a halmozottan hátrányos helyzet fennállása esetén a jogosultak 6.500,- Ft pénzbeli támogatásban részesültek. Arra a gyermekekre vonatkozóan, akire csak a rendszeres gyermekvédelmi kedvezményre való jogosultság került megállapításra csupán 6.000,- Ft

összegű pénzbeli támogatásban részesültek. A kifizetésre kerülő összeg nem az önkormányzat költségvetését terheli, 100%-ban állami finanszírozás, melyet a központi költségvetés biztosít. A hátrányos, illetve halmozottan hátrányos helyzetű gyermekeket egyéb kedvezmények is megilletik, ezen kedvezmények főleg az óvodában illetve nagyobb részük az iskolában vehető igénybe például az alapfokú művészeti oktatás ingyenessége, vagy továbbtanulás esetén a felvételi pontoknál plusz pontszámot jelent.

Szikszo Város területén a 2019-es évben az alábbi hátrányos, halmozottan hátrányos helyzet megállapítására került sor:

2019-es évben	gyermekek száma
hátrányos helyzet megállapítása	96 fő
halmozottan hátrányos helyzet megállapítása	117 fő

Gyermek és fiatal felnőtt rászorultságára tekintettel nyújtott pénzbeli támogatás:

A segélyezési rendszer keretében is sor kerül a gyermekek támogatására rendkívüli települési támogatás formájában. Elsősorban azon gyermekek/családok részére került ilyen támogatás megállapításra, akik önhibájukon kívül kerültek nehéz anyagi helyzetbe. A támogatás megállapítása során folyamatos kapcsolattartás történik a családsegítő szolgálat munkatársával, szükség esetén környezettanulmány elvégzésére is sor kerül. A rendkívüli települési támogatás alkalmanként jelentkező, a megélhetést veszélyeztető többletkiadások viseléséhez nyújtott támogatás. Rendkívüli települési támogatás gyermekre tekintettel az alábbi szempontok miatt kerültek megállapításra: élelmiszerre, ruhaneműre, tüzelőre, krónikus, hosszantartó betegségből eredő kórházi kezelés esetén, gyógyszerre, nagyobb balesetre, gyógyászati segédeszközre, szemüvegre, iskoláztatással kapcsolatos költségek rendezésére. Az önkormányzat célja a hátránnyal küzdő családok megsegítése, a hátrányok leküzdése.

Településünk a továbbtanuló helyi lakosokat a Bursa Hungarica ösztöndíj programban való részvétellel támogatja. Ennek keretén belül 31 fő, 1.550.000-Ft összegű támogatása valósult meg az elmúlt évben.

3. A gyermekétkeztetés megoldásának módjai, kedvezményben részesülőkre vonatkozó statisztikai adatok

A gyermekétkeztetéssel kapcsolatos feladatokat az önkormányzat az óvodában, az iskoláskorú gyermek számára az iskolai menzán történő étkeztetéssel biztosítja. Az alsó tagozaton lehetőség van napi háromszori étkezés – tízórai, ebéd, uzsonna – igénybevételére, valamint egyszeri fő étkezés igénybevételére is a szülők igényei szerint. A felső tagozaton egyszeri főétkezés igénybevételére van lehetőség.

Szünidei gyermekétkeztetés

A gyermekek védelméről és a gyámügyi igazgatásról szóló 1997. évi XXXI. törvény szabályozása alapján a települési önkormányzatok kötelezően ellátandó feladatként biztosítják a szünidei gyermekétkeztetést, amelynek keretében a szülő kérelmére a települési önkormányzatnak napi egyszeri melegételt kell biztosítani a hátrányos helyzetű illetve halmozottan hátrányos helyzetű gyermek részére 5 hónapos kortól 18 éves korig a tanév rendjéről szóló EMMI rendeletben meghatározott iskolai szünidő, valamint az óvoda és bölcsőde ezen időszakoknak megfelelő zárva tartási időtartamára eső munkanapokon ide értve azokat a gyermekeket is, akik nem rendelkeznek intézményi – bölcsődei, óvodai vagy iskolai

tanulói jogviszonnyal. A szünidei étkeztetés megkezdése előtti hetekben felhívást teszünk közzé a Szikszói Közös Önkormányzati Hivatal hirdetőtábláján és az oktatási intézmények (óvodák, iskolák) hirdető tábláin papír alapon.

Minden szünidő előtt tájékoztatjuk az érintett családokat az igénybevétel feltételeiről és lehetőségéről, mert sajnos tapasztaljuk, hogy hajlamosak a szülők elfeledkezni a nyilatkozatok kitöltéséről. Ezáltal figyelemmel tudjuk kísérni, hogy a rászorulóknak minél nagyobb arányban vegyék igénybe a lehetőséget. A Szikszói Közös Önkormányzati Hivatal a tájékoztatót megküldi a jogosultak részére, majd ezt követően a Szikszói Kistérségi Szociális Szolgáltató Központ munkatársai keresik fel az érintetteket – hivatalunk által biztosított felkérés és névsor alapján – szóban tájékoztatják őket, valamint segítséget nyújtanak az igényfelmérésben, a nyilatkozatok kitöltésében annak érdekében, hogy minél több jogosult gyermek vegye igénybe a szünidei étkeztést.

Szikszó Város Önkormányzata nagyon jó lehetőségnek találja, hogy a hátrányos és halmozottan hátrányos gyermekek részére lehetőség nyílik a szünidei gyermekétkeztetés igénybevételére. Szikszón is - ahogyan más településeken is - nagyon magas a szociális segélyben részesülőknek a száma és egyre gyakrabban tapasztaljuk azt, hogy a rendkívüli települési támogatás megállapítása iránt benyújtott kérelmekben sokan azt fogalmazzák meg, hogy olyan anyagi körülmények között élnek melyben gyermekeik étkeztetését, ruháztatását, a gyógyszerek megvásárlását, a közüzemi számlák kifizetését nem tudják biztosítani. A tapasztalat szerint már többen veszik igénybe, mint az előző években, mert korábban csak helyben fogyasztással vehették igénybe a szünidei étkeztetést. A szülők elmondása szerint a gyerekek szégyellték, megalázóan tartották a helyben történő ételfogyasztást. Ezen tapasztalatok alapján döntött úgy önkormányzatunk, hogy lehetőséget biztosít arra, hogy elvitellel is igénybe vehető legyen a szünidei gyermekétkeztetés. Szikszó Város Önkormányzata együttműködési megállapodást kötött a ZTR. Közétkeztető Kft.-vel arra vonatkozóan, hogy az elnyert támogatási összeg biztosításával az étkeztetés közvetlen megvalósulását a ZTR. Közétkeztető Kft. látja el. Az étkeztetésben részt vevő gyermek előre nem látható hiányzása (betegség, egyéb akadályoztatása) esetén a számára biztosított és elkészített étel az étkeztetésben részt vevő gyermekek számára átadható. Az elmúlt években nagyon alacsony volt a részvételi hajlandóság a szünidei étkeztetés iránt, ezért azóta sokkal nagyobb hangsúlyt fektetünk arra, hogy a jogosult gyermekek szülei jobban figyeljenek oda ennek a lehetőségnek az igénybevételére. Ezt a már fentebb említett Szikszói Kistérségi Szociális Szolgáltató Központ munkatársai és a közmunkaprogramban dolgozó munkavezetők segítségével próbáljuk megoldani, mivel a jogosult gyermekek szülei nagyrészt közmunkások.

Az étkeztetésben résztvevők száma a 2019-es évben:

Tavaszi	Nyári	Őszi	Téli
75 fő	106 fő	66 fő	54 fő

4. Az önkormányzat által biztosított személyes gondoskodást nyújtó ellátások bemutatása

4.1. A gyermekjóléti szolgáltatás biztosítása

A gyermekjóléti szolgáltatást az önkormányzat a Szikszói Kistérségi Szociális Szolgáltató Központ által fenntartott Család-és Gyermekjóléti Szolgálat útján biztosítja.

4.2. Gyermek napközbeni ellátásának módja

Az önkormányzat ezen feladatát, a törvény alapján a közoktatási törvény hatálya alá tartozó óvodában és iskolákban történő elhelyezéssel látja el.

4.3. Bölcsődei ellátás

A bölcsődei ellátást településünkön a Szikszói Városi Óvoda és Bölcsőde látja el. A törvény előírja, hogy olyan településen ahol 21 fő igényli a bölcsődei ellátást, ott kötelező bölcsődei csoportot indítani. A településen élő kisgyermekes családok gondjait nagyon megkönnyíti a bölcsődei ellátás biztosítása, mert városunkban sok olyan kisgyermekes család él, ahol az anyukák jó részét visszavárják a munkahelyükre. A 2019-es évben 12 gyermek vett részt a bölcsődei ellátásban.

5. A gyermekjóléti szolgáltatás biztosításának módja, működésének tapasztalata (alapellátásban részesülők száma, gyermekek veszélyeztetettségének okai, válsághelyzetben levő várandós anyák gondozása, családjából kiemelt gyermek szüleinek gondozása, jelzőrendszer tagjaival való együttműködés tapasztalatai), gyermekek napközbeni ellátásának, gyermekek átmeneti gondozásának biztosítása, ezen ellátások igénybevétele, s az ezzel összefüggő tapasztalatok

A gyermekjóléti szolgáltatást az önkormányzat a Szikszói Kistérségi Szociális Szolgáltató Központ által fenntartott Család- és Gyermekjóléti Szolgálat útján biztosítja. A Szolgálat külön beszámolóban ad tájékoztatást az intézményben folyó munkáról. A Szikszói Kistérségi Szociális Szolgáltató Központ által készített és már a képviselő-testület által elfogadott részletes beszámoló a Kormányhivatal részére jelen beszámoló mellékletként kerül felterjesztésre.

A gyermekjóléti szolgáltatásokat biztosító intézményegységek éves munkájának összegzéseként elmondható, hogy az intézmény által ajánlott programokat az ellátási területeken lévő óvodák, iskolák szívesen fogadják, sokszor ötletet is adnak, hogy milyen típusú foglalkozásokra lenne szüksége, igénye a gyerekeknek. A meghirdetett foglalkozásokon a gyermekek örömmel vesznek részt. A gyermekjóléti szolgálat tapasztalata szerint a legfőbb probléma, hogy a szegénység mellett a szülők felelőtlen viselkedése miatt a gyermek/család is nehéz anyagi helyzetbe kerül. A szülők elveszítik a családi pótlékot az iskolai hiányzások miatt, amely további terhet, nehézséget megélhetési, problémákat okoz a családoknak.

A Védőnői Szolgálat 2019-ben folytatott gyermekvédelmi tevékenységéről:

Szikszón az 1-es körzetben 2019 év december 31-én 195 gyermek gondozott volt nyilvántartva, 2-es körzetben 189 gyermek. A szociális veszélyeztetettség az 1-es körzetben 71 gyermeket érintett a 2-es körzetben 57 gyermeket. Családlátogatások 2019-ben az 1-es körzetben 768, a 2-es körzetben 909 alkalommal történtek. 2019-ben 9 esetben történt írásos megkeresés a Gyermekjóléti Szolgálat felé.

Területi védőnői gondozás összefoglalása 2019. 12. 31. állás szerint.

	Gondozott családok száma	Gondozott 0-7 évesek száma	Gondozott 0-14 évesek száma	Veszélyeztetettek száma (egészségügyi és szociális okból)
1-es körzet	175	195	n.a.	71
2-es körzet	109	189	n.a.	57

A családlátogatások száma: 2019-ben Szikszó 1-es körzetében 768 alkalom, 2-es körzetében 909 alkalommal

Várandósgondozás

2019-ben várandós gondozások száma:

1-es körzet: 54 várandós gondozás, amelyből 10 esetben szociális okból veszélyeztetett.

2-es körzet: 40 várandós gondozás, amelyből 3 esetben szociális okból veszélyeztetett.

6. A felügyeleti szervek által gyámhatósági, gyermekvédelmi területen végzett szakmai ellenőrzések tapasztalatainak, továbbá a gyermekjóléti és gyermekvédelmi szolgáltató tevékenységet végzők ellenőrzésének alkalmával tett megállapítások bemutatása

A Borsod-Abaúj-Zemplén Megyei Kormányhivatal szakmai ellenőrzést a 2019-es évben nem végzett.

7. Jövőre vonatkozó javaslatok, célok meghatározása a Gyvt. előírásai alapján (milyen ellátásokra és intézményekre lenne szükség a problémák hatékonyabb kezelése érdekében, gyermekvédelmi prevenció elképzelések)

Az önkormányzat a jövőre vonatkozóan is célul tűzi ki még több intézménnyel, civil szervezetekkel való együttműködést. A probléma és a hátrányok csökkentése érdekében fontos a folyamatos kapcsolattartás, kommunikáció a nemzetiségi önkormányzatok képviselőivel. Az önkormányzat minden éven arra törekszik, hogy a hátránnyal küzdő rendszeres gyermekvédelmi kedvezményben részesülő gyermekek részére több napos teljesen ingyenes tábort biztosítson. Célja ezzel, hogy kikapcsolódási, és szabadidős tevékenységet biztosítson olyan gyermekek részére, akik anyagi okok miatt nem jutnak el nyaralni. A tavalyi évben az önkormányzat Tiszafüredre szervezte meg a tábort ezen gyermekek részére, amely négy nap volt és teljesen ingyenes. A gyermekek ezen táborokat már nagyon várják, mindig aktívak és érdeklődők minden program iránt. A táborokat az önkormányzat már harmadik alkalommal pályázati pénzből tudja megvalósítani.

Minden egyes gyermek, illetve öt nevelő család problémája komplex gondolkodást igényel. Ehhez szükséges a gyermekjóléti szolgálat, a gyámhatóság és a jegyzői gyámhatóság közötti szoros együttműködés, minden lehetséges segítségforma biztosítása érdekében. Törekedni kell ennek a kapcsolatnak az életben tartására, az ügyintézők közötti személyes, helyismereten alapuló információ áramoltatására, szem előtt tartva a helyi Gyermekjóléti Szolgálat

felelősségét ebben az igazgatási rendszerben.

8. A bűnmegelőzési program főbb pontjainak bemutatása (amennyiben a településen készült ilyen program), valamint a gyermekkorú és a fiatalkorú bűnelkövetők számának az általuk elkövetett bűncselekmények számának, a bűnelkövetés okainak bemutatása

A Szikszói Kistérségi Szociális Szolgáltató Központ a 2019-es évben ismételtén megszervezte a járás összes iskolájában a „Vigyázz magadra” című programot, mely során az általános iskolák felső tagozatos tanulói a bűncselekmények fogalmaival, büntetési tételeivel és hosszútávú következményeivel gyarapíthatták tudásukat. A gyermekek mókás feladatok alapján sajátították el a közlekedés szabályait, majd ezzel kapcsolatban rajzverseny is került meghirdetésre.

9. A települési önkormányzat és a civil szervezetek közötti együttműködés keretében milyen feladatok, szolgáltatások ellátásában vesznek részt civil szervezetek (alapellátás, szakellátás, szabadidős programok, drogprevenció stb.)

Városunkban jelenleg az önkormányzat és a civil szervezetek között folyamatos kapcsolattartás van, amelynek keretében szabadidős programok, sport, és kulturális programok kerülnek megrendezésre. A településen sokrétű civil munka folyik, a tevékenységi körök széles spektruma, a szociális, ifjúsági, kulturális, művészeti és óvodai, iskolai alapítványokon és sportegyesületeken keresztül sok-sok ember önkéntes munkájához biztosítanak keretet, jogi formát. A településen élénk, aktív civil élet folyik, amely a társadalom minden területét érinti. A civil szervezetek új szint visznek a város életébe, közösségi akciókkal erősítik a település lakosságának lokálpatriotizmusát. A helyi civil szervezetek fontos szerepet töltenek be a helyi társadalom közösségformálásában, a helyi identitástudat erősítésében. A településen tevékenykedő civil szervezetek működéséhez, illetve az általuk szervezendő eseményekhez Szikszó Város Önkormányzat Polgármestere a Mecénás Alapból eseti jelleggel, egyedi elbírálás alapján biztosít anyagi forrást. Jellemzően azonban minden szervezet saját maga teremti elő a működéséhez szükséges forrást, sikerrel pályázva különböző támogatási alapokhoz. Az alábbi civil szervezetek segítségével valósulnak meg a szikszói gyermekek szabadidőjének hasznos eltöltése:

Hell Fight Club Küzdősport Egyesület, Oroszlánszív Küzdősport Egyesület, Szent Márton Katolikus Gimnázium és Ált. Isk., Szikszói Móricz Zsigmond Ált.Isk., Abaúj TV, Református Egyház Község, Szikszói Görögkatolikus Parókia, Római Katolikus Plébánia Egyesület, a Szikszói Polgárőr Egyesület, Roma Kötelék Egyesület, Zenével az Ifjú Tehetségekért Alapítvány, Bethánia Napköziotthonos Óvoda, Szikszói Városi Óvoda és Bölcsőde, Miskolci Tankerület Központ, Szikszói Állatbarát Alapítvány, Borsod-Abaúj Zemplén Megyei Sakkszövetség

Szikszó, 2020. május 29.

Battáné dr. Tóth Zita sk.
jegyző



Szikszó Város Önkormányzata
3800 Szikszó, Kálvin tér 1.
Tel:(46) 596-450; Fax:(46) 596-211
info@szikszo.hu

HATÁROZAT

16/2020.(V.29.) Szikszó Város Önkormányzat Polgármesteri Határozata

Szikszó Város Önkormányzat Polgármestere a veszélyhelyzet kihirdetéséről szóló 40/2020. (III.11.) számú kormányrendelet, valamint a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény 46.§ (4) bekezdésében foglalt jogköre alapján a Képviselő-testület feladat- és hatáskörében eljárva az alábbiak szerint határoz:

Döntés Szikszó Város Önkormányzata Adatvédelmi és adatbiztonsági szabályzatának elfogadásáról

Szikszó Város Önkormányzat Polgármestere úgy határoz, hogy 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 (EU) 2016/679 rendelet (Általános adatvédelmi rendelet vagy GDPR) és az Információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény alapján elfogadja a határozat mellékletét képező „Adatvédelmi és adatbiztonsági szabályzat”-ot Szikszó Város Önkormányzatára vonatkozóan.

(Írásos anyag csatolva: 3. sz. melléklet)

Felelős: polgármester

Határidő: azonnal

Kelt: Szikszó, 2020.05.29.





Szikszó Város Önkormányzata

3800 Szikszó, Kálvin tér 1.

ADATVÉDELMI ÉS ADATBIZTONSÁGI SZABÁLYZAT

Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.)
a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről
és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről
(általános adatvédelmi rendelet) szerint

érvényes:

2020.05.29

jóváhagyta:


Sváb Antal Béla

Tartalomjegyzék

Vezetői nyilatkozat.....	4
Adatkezelő/adatfeldolgozó adatai	5
1. A személyes adatok kezelésére vonatkozó általános elvek	6
1.0. Áttekintés az Európai Parlament és a Tanács (EU) 2016/679 rendeletéről	6
1.1. Az Adatvédelmi és adatbiztonsági szabályzat célja	6
1.2. Az Adatvédelmi és adatbiztonsági szabályzat hatálya	7
1.3. Kapcsolódó jogforrások, egyéb szabályzatok	7
1.4. A személyes adatok kezelésére vonatkozó elvek	8
1.5. Az adatkezelés jogszerűsége	9
1.6. Különleges adatok (a személyes adatok különleges kategóriáinak) kezelése.....	9
1.7. Bizonyítható hozzájárulás.....	10
1.8. Az érintett jogai	11
1.9. Felelősségi körök, Szervezet vezetőjének feladatai.....	13
1.10. Adatvédelmi tisztviselő.....	14
1.11. Képzés.....	14
2. A szervezet adatvédelmi feladatai	15
2.1. Adatvédelmi tisztviselő kijelölése	15
2.2. Adatkezelési, adatfeldolgozói tevékenységek nyilvántartása	16
2.3. Átlátható tájékoztatás, kommunikáció és az érintett jogainak gyakorlására vonatkozó intézkedések.....	17
2.3.1. Tájékoztatás és a személyes adatokhoz való hozzáférés joga.....	18
2.3.2. Az érintett hozzáférési joga	19
2.3.3. Az érintett helyesbítéshez való joga	20
2.3.4. A törléshez, elfeledtetéshez való jog	20
2.3.5. Az adatkezelés korlátozásához való jog	21
2.3.6. A személyes adatok helyesbítéséhez vagy törléséhez, illetve az adatkezelés korlátozásához kapcsolódó értesítési kötelezettség	22
2.3.7. Az adathordozhatósághoz való jog.....	22
2.3.8. A tiltakozáshoz való jog	22
2.3.9. Automatizált döntéshozatal egyedi ügyekben, profilalkotás.....	22
2.3.10. A személyes adatokkal összefüggő jogok érvényesítése az érintett halálát követően.....	23
2.4. Az érintetti kérelmek kezelése	23
2.5. Az adatkezelés biztonsága, technikai és szervezési intézkedések végrehajtása	24
2.6. Az adatvédelmi incidensek.....	25
2.6.1. Incidensek belső nyilvántartása.....	25
2.6.2. Incidens NAIH bejelentése	25
2.6.3. Érintettek tájékoztatása az Incidensről.....	26
2.6.4. Adatvédelmi incidensek kezelése	26
2.7. Érdemérlegelés	27
2.8. Adatközlés, adattovábbítás, nyilvánosságra hozatal.....	28
2.8.1. Adattovábbítás harmadik országokba	29
2.9. Adatfeldolgozás, adatfeldolgozói garancianyújtás.....	29
2.10. Kötelező adatkezelések felülvizsgálata.....	31
2.11. Adatvédelmi hatásvizsgálat.....	32
3. Személyes adatok kezelése, nyilvántartása	33
3.1. Munkavállalók adatkezelései	33
3.2. Ügyfelekkel, szakfeladatokkal kapcsolatos adatkezelések	35

3.2.1.	Okmánymásolás	36
4.	Technikai és szervezési intézkedések	37
4.1.	Adminisztratív védelmi intézkedések.....	37
4.2.	Fizikai védelmi intézkedések	40
4.3.	Logikai védelmi intézkedések	41
4.4.	Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény hatálya alá tartozó szervek további követelményei	45
	Fogalomtár	46

Verzió: v1.01

Vezetőinyilatkozat

A Szikszó Város Önkormányzata (továbbiakban Szervezet) vezetőjeként hatályba léptetem jelen Adatvédelmi és adatbiztonsági szabályzatot, annak érdekében, hogy a Szervezet alkalmazza az Európai Parlament és a Tanács (EU) 2016/679 rendeletét (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 (továbbiakban Rendelet) előírásait, figyelembe véve az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény 2. § (2) bekezdése alapján vonatkozó rendelkezéseit.

A Szikszó Város Önkormányzata vezetője megismerve a GDPR által támasztott kihívásokat, elkötelezett aziránt, hogy a Szervezet az adatvédelmi szabályoknak megfeleljen, felelős jelen Adatvédelmi és adatbiztonsági szabályzat folyamatos karbantartásáért és az abban foglaltak végrehajtásáért.

A szabályzat a GDPR előírásait követve, a Szervezet minden telephelyén, szervezeti egységén, munkaterületén, minden tevékenységére rögzíti a személyes adatok kezelésére vonatkozó előírásokat, eljárásokat, és egyértelműen meghatározza a kapcsolódó dokumentált információs rendszert.

A Szervezet biztosítja a Rendelet és jelen szabályzat elvárásainak teljesítéséhez szükséges anyagi és személyi erőforrásokat.

2020.05.29



Sváb Antal Béla

Adatkezelő/adatfeldolgozó adatai

Adatkezelő, adatfeldolgozó neve: Szikszó Város Önkormányzata

Címe (hivatalos levelezési cím): 3800 Szikszó, Kálvin tér 1.

Honlapjának elérhetősége: <http://www.szikszo.hu>

Telefonszáma: +36 46 596-444

Adószáma: 15725723-2-05

Képviselője neve: Sváb Antal Béla

Adatkezelési tájékoztató elérhetősége: 3800 Szikszó, Kálvin tér 1.

Adatvédelmi tisztviselő neve: Juhász Gergely

Adatvédelmi tisztviselő elérhetősége: adatvedelem@szikszo.hu

Nyilatkozat Adatvédelmi tisztviselő kijelöléséről:

Adatvédelmi tisztviselő kijelölésére kerül sor, mert:

- Az adatkezelést közhatalmi szervek vagy egyéb, közfeladatot ellátó szervek végzik, kivéve az igazságszolgáltatási feladatkörükben eljáró bíróságokat

1. A személyes adatok kezelésére vonatkozó általános elvek

1.0. Áttekintés az Európai Parlament és a Tanács (EU) 2016/679 rendeletéről

2016. május 25-én lépett hatályba és 2018. május 25-től kötelezően alkalmazandó az Európai Unió valamennyi tagállamában az új európai adatvédelmi rendelet (az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet, Rendelet). A Rendelet a természetes személyeknek a személyes adatok kezelése tekintetében történő védelmére és a személyes adatok szabad áramlására vonatkozó szabályokat állapít meg.

A rendeletet kell alkalmazni a személyes adatoknak az Unióban tevékenységi hellyel rendelkező adatkezelők vagy adatfeldolgozók tevékenységeivel összefüggésben végzett kezelésére, függetlenül attól, hogy az adatkezelés az Unió területén történik vagy nem, valamint ha az adatkezelés az Unióban tartózkodó érintettek személyes adatainak kezelésre irányul, akkor is, ha az Unióban az adatkezelő vagy az adatfeldolgozó tevékenységi hellyel nem rendelkezik.

1.1. Az Adatvédelmi és adatbiztonsági szabályzat célja

Az adatkezelőnek, adatfeldolgozónak belső adatvédelmi szabályokat kell alkalmaznia a személyes adatok védelmének biztosítása céljából megvalósított technikai és szervezési intézkedések részeként, ha ez az adatkezelési tevékenység vonatkozásában arányos.

A közfeladatot ellátó szerv az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Infotv.) szerinti kötelezően közzéteendő közérdekű adatok közzétételi kötelezettségét jelen szabályzat hatályos és teljes szövegének közzétételével teljesíti.

Jelen szabályzat célja a hatálya alá tartozó tárgykörökben az adatok kezelésére vonatkozó alapvető szabályok meghatározása annak érdekében, hogy a természetes személyek magánszféráját az adatkezelő, munkavállalói vagy egyéb, munkavégzésre irányuló jogviszony alapján foglalkoztatott személyek, illetőleg a szerződéses kapcsolatban álló partnerek vagy más harmadik természetes személyek által tiszteletben tartásuk, minden adatkezelési folyamat, munkavégzés, közfeladat teljesítése során a meghatározott adatkezelési célból, a szervezet részére átadott személyes adataik kezelése, továbbítása, feldolgozása, tárolása során biztosítva legyen az adatalanyok információs önrendelkezési jogának maradéktalan érvényesülése, törvényes érdekeik és jogaik védelme, az adatok kezelésének jogszerű célhoz rendelése és a felhasználás alatt mindvégig e célhoz kötöttsége.

Az Adatvédelmi és adatbiztonsági szabályzat további célja, hogy meghatározza a működés során az adatkezeléssel kapcsolatos nyilvántartások vezetésének törvényes rendjét, biztosítsa az adatvédelem alkotmányos elveinek, az információs önrendelkezési jognak az érvényesülését, valamint hogy a személyes adatok kezelése a jogszabályokban előírtaknak megfelelően történjen.

Az adatalanyi minőség - és ezáltal az adatvédelmi szabályoknak történő megfelelés követelménye - a személyes adat jogszerű módon történő megszerzésétől kezdődően, az adott jogviszony létrehozásán keresztül annak fennállása alatt és azt követően is fennáll mindaddig, amíg az adott adatalanyal összefüggésben a személyes adatok végleges és visszafordíthatatlan módon történő törlése - vagy ahol az lehetséges, illetve szükséges, a megsemmisítése - végrehajtásra nem kerül.

1.2. Az Adatvédelmi és adatbiztonsági szabályzat hatálya

A Szikszó Város Önkormányzata (továbbiakban Szervezet) jelen Adatvédelmi és adatbiztonsági szabályzatának hatálya valamennyi olyan szervezeti egységére, telephelyére kiterjed, amely részt vesz a keletkezett, feldolgozott, tárolt, illetve továbbított személyes adatok kezelésében, valamennyi munkatársra, munkavégzésre irányuló jogviszony alapján foglalkoztatott személyre, szerződéses kapcsolatban álló partnerre, akik a szervezet által használt rendszerekhez és az azokban tárolt személyes adatokhoz hozzáféréssel rendelkeznek, illetve akik részt vesznek a szervezetnél keletkezett, feldolgozott, tárolt, illetve továbbított személyes adatok kezelésében.

A szerződéses partnerekkel, harmadik felekkel szembeni elvárásokat, kötelezettségeket a tevékenységet képező, jogviszonyt megalapozó szerződésekben, megállapodásokban kell érvényesíteni. Meg kell ismertetni a szerződéses partnerekkel, harmadik felekkel az adatkezelésre, titoktartási kötelezettségekre vonatkozó felételeket.

Egyéni vállalkozó, egyéni cég, őstermelő magánszemély e szabályzat alkalmazásában természetes személynek minősül, így adataik kezelése kapcsán személyes adatkezelés történik.

A szabályzat a kiadás napján lép hatályba, mellyel a korábbi ezzel kapcsolatos szabályzat hatályát veszti.

A Szabályzatot az adatkezelések körülményeiben beállt lényeges változások esetén, de legalább 3 évenként felül kell vizsgálni

1.3. Kapcsolódó jogforrások, egyéb szabályzatok

- Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (a továbbiakban: Rendelet)
- Magyarország Alaptörvénye (2011. április 25.)
- 2011. évi CXII. törvény az információs önrendelkezési jogról és információszabadságról (Infotv.),
- 2013 évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (Ibtv.)
- 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről
- 2005. évi CXXXIII. törvény a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól (Szvtv.)
- 1999. évi LXIII. törvény a közterület-felügyeletről (Kftfv.)
- 2011. évi CLXV. törvény a polgárőrségről és a polgárőri tevékenység szabályairól
- 1994. évi XXXIV. törvény a Rendőrségről (Rtv.)
- 2012. évi I. törvény a munka törvénykönyvéről (Mt.)
- 2011. évi CXCIX. törvény a közszolgálati tisztviselőkről (Ktv.)
- 1992. évi XXXIII. törvény a közalkalmazottak jogállásáról
- 2013. évi V. törvény a polgári törvénykönyvről (Ptk.)
- 2011. évi CXCV. törvény az államháztartásról
- 2011. évi CLXXXIX. törvény Magyarország helyi önkormányzatairól
- 1991. évi XX. törvény a helyi szervezet, intézmények és szerveik, a köztársasági megbízottak, valamint egyes centrális alárendeltségű szervek feladat- és hatásköreiről

- 2017. évi I. törvény a közigazgatási perrendtartásról
- 1995. évi CXVII. törvény a személyi jövedelemadóról (Szja.)
- 2017. évi CL. törvény az adózás rendjéről (Art.)
- 1997. évi LXXXI. törvény a társadalombiztosítási nyugellátásról
- 2000. évi C. törvény a számvitelről (Sztv.)
- 2017. évi LIII. törvény a pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról (Pmt.)
- NAIH ajánlások: <https://www.naih.hu/ajanlasok.html>
- 29-Adatvédelmi Munkacsoport dokumentumai: <https://naih.hu/29--adatvedelmi-munkacsoport-dokumentumai.html>
- **Kapcsolódó főbb belső szabályzatok:**
 - Informatikai biztonsági szabályzat (az lbtv. hatálya alá tartozó szervezeteknek, többek között a helyi és a nemzetiségi önkormányzatok képviselő-testületének hivatalainak, a hatósági igazgatási társulásoknak, valamint ezen szervek számára adatkezelést végzőknek)
 - Közszolgálati szabályzat (Ktv. hatálya alá tartozó szervezeteknek)

1.4. A személyes adatok kezelésére vonatkozó elvek

1. **Jogszerűség, tisztességes eljárás és átláthatóság:** A személyes adatok kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni.
2. **Célhoz kötöttség:** A személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történjen, és azokat ne kezeljék ezekkel a célokkal össze nem egyeztethető módon. Nem minősül az eredeti céllal össze nem egyeztethetőnek a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból történő további adatkezelés.
3. **Adattakarékosság:** A személyes adatok az adatkezelés céljai szempontjából megfelelőek és relevánsak kell, hogy legyenek, és a szükségesre kell korlátozódniuk.
4. **Pontosság:** A személyes adatoknak pontosnak és szükség esetén naprakésznek kell lenniük. Minden ésszerű intézkedést meg kell tenni annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul töröljék, vagy helyesbítsék.
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 kezelésére közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból kerül majd sor, az érintettek jogainak és szabadságainak védelme érdekében előírt megfelelő technikai és szervezési intézkedések végrehajtására is figyelemmel.
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.
7. **Elszámoltathatóság:** Az adatkezelő felelős a fenti alapelveknek való megfelelésért, továbbá képesnek kell lennie e megfelelés igazolására.

1.5. Az adatkezelés jogszerűsége

A Rendelet hat lehetséges jogalapot tartalmaz azon személyes adatok kezelése tekintetében, amelyek nem tartoznak a személyes adatok különleges kategóriájába (pl. egészségügyi, biometrikus vagy genetikai adatok).

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.

1.6. Különleges adatok (a személyes adatok különleges kategóriáinak) kezelése

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 kezelése tilos, a különleges adatok kezelése csak a felsorolt esetekben lehetséges:

- a) az érintett kifejezett hozzájárulását adta az említett személyes adatok egy vagy több konkrét célból történő kezeléséhez, kivéve, ha az uniós vagy tagállami jog úgy rendelkezik, hogy a tilalom nem oldható fel az érintett hozzájárulásával;
- b) az adatkezelés az adatkezelőnek vagy az érintettnek a foglalkoztatást, valamint a szociális biztonságot és szociális védelmet szabályozó jogi előírásokból fakadó kötelezettségei teljesítése és konkrét jogai gyakorlása érdekében szükséges, ha az érintett alapvető jogait és érdekeit védő megfelelő garanciákról is rendelkező uniós vagy tagállami jog, illetve a tagállami jog szerinti kollektív szerződés ezt lehetővé teszi;
- c) az adatkezelés az érintett vagy más természetes személy létfontosságú érdekeinek védelméhez szükséges, ha az érintett fizikai vagy jogi cselekvőképtelensége folytán nem képes a hozzájárulását megadni;
- d) az adatkezelés valamely politikai, világnézeti, vallási vagy szakszervezeti célú alapítvány, egyesület vagy bármely más nonprofit szervezet megfelelő garanciák mellett végzett jogszerű tevékenysége keretében történik, azzal a feltétellel, hogy az adatkezelés kizárólag az ilyen szerv jelenlegi vagy volt tagjaira, vagy olyan személyekre vonatkozik, akik a szervezettel rendszeres kapcsolatban állnak a szervezet céljaihoz kapcsolódóan, és hogy a személyes adatokat az érintettek hozzájárulása nélkül nem teszik hozzáférhetővé a szervezeten kívüli személyek számára;

- e) az adatkezelés olyan személyes adatokra vonatkozik, amelyeket az érintett kifejezetten nyilvánosságra hozott;
- f) az adatkezelés jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez szükséges, vagy amikor a bíróságok igazságszolgáltatási feladatkörükben járnak el;
- g) az adatkezelés jelentős közérdek miatt szükséges, uniós jog vagy tagállami jog alapján, amely arányos az elérni kívánt céllal, tiszteletben tartja a személyes adatok védelméhez való jog lényeges tartalmát, és az érintett alapvető jogainak és érdekeinek biztosítására megfelelő és konkrét intézkedéseket ír elő;
- h) az adatkezelés megelőző egészségügyi vagy munkahelyi egészségügyi célokból, a munkavállaló munkavégzési képességének felmérése, orvosi diagnózis felállítása, egészségügyi vagy szociális ellátás vagy kezelés nyújtása, illetve egészségügyi vagy szociális rendszerek és szolgáltatások irányítása érdekében szükséges, uniós vagy tagállami jog alapján vagy egészségügyi szakemberrel kötött szerződés értelmében (ha ezen adatok kezelése olyan szakember által vagy olyan szakember felelőssége mellett történik, aki uniós vagy tagállami jogban, illetve az arra hatáskörrel rendelkező tagállami szervek által megállapított szabályokban meghatározott szakmai titoktartási kötelezettség hatálya alatt áll, illetve olyan más személy által, aki szintén uniós vagy tagállami jogban, illetve az arra hatáskörrel rendelkező tagállami szervek által megállapított szabályokban meghatározott titoktartási kötelezettség hatálya alatt áll);
- i) az adatkezelés a népegészségügy területét érintő olyan közérdekből szükséges, mint a határokon át terjedő súlyos egészségügyi veszélyekkel szembeni védelem vagy az egészségügyi ellátás, a gyógyszerek és az orvostechikai eszközök magas színvonalának és biztonságának a biztosítása, és olyan uniós vagy tagállami jog alapján történik, amely megfelelő és konkrét intézkedésekről rendelkezik az érintett jogait és szabadságait védő garanciákra, és különösen a szakmai titoktartásra vonatkozóan;
- j) az adatkezelés a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból szükséges olyan uniós vagy tagállami jog alapján, amely arányos az elérni kívánt céllal, tiszteletben tartja a személyes adatok védelméhez való jog lényeges tartalmát, és az érintett alapvető jogainak és érdekeinek biztosítására megfelelő és konkrét intézkedéseket ír elő.

A tagállami jog különös rendelkezéseket állapíthat meg az adatok védelmére vonatkozóan annak érdekében, hogy kiigazítsák a Rendeletben foglalt szabályok alkalmazását valamely jogi kötelezettségnek való megfelelés vagy közérdekből végzett feladat végrehajtása vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlása tekintetében.

1.7. Bizonyítható hozzájárulás

Ha az adatkezelés az érintett hozzájárulásán alapul, az adatkezelőnek kell tudni bizonyítania, hogy az adatkezelési művelethez az érintett hozzájárult. A hozzájárulás önkéntességének megállapításához figyelembe kell venni többek között azt a ténytet, hogy a szerződés teljesítésének – beleértve a szolgáltatások nyújtását is – feltételül szabták-e az olyan személyes adatok kezeléséhez való hozzájárulást, amelyek nem szükségesek a szerződés teljesítéséhez.

Különösen a más ügyben tett írásbeli nyilatkozattal összefüggésben garanciákkal szükséges biztosítani azt, hogy az érintett tisztában legyen azzal a ténnyel, hogy hozzájárulását adta, valamint azzal, hogy ezt milyen mértékben tette. Egy hozzájárulás egy adatkezelési cél érdekében végzett adatkezeléshez való hozzájárulást jelent. Az adatkezelő lehetőség szerint előre megfogalmazott hozzájárulási nyilatkozatról

gondoskodik, amelyet érthető és könnyen hozzáférhető formában bocsát rendelkezésre, nyelvezetének, pedig világosnak és egyszerűnek kell lennie, és nem tartalmazhat tisztességtelen feltételeket.

Ahhoz, hogy a hozzájárulás tájékoztatáson alapulónak minősüljön, az érintettnek legalább tisztában kell lennie az adatkezelő kilétével és a személyes adatok kezelésének céljával.

A hozzájárulás megadása nem tekinthető önkéntesnek, ha az érintett nem rendelkezik valós vagy szabad választási lehetőséggel, és nem áll módjában a hozzájárulás anélküli megtagadása vagy visszavonása, hogy ez kárára válna.

Az érintett jogosult arra, hogy hozzájárulását bármikor visszavonja. A visszavonás nem érinti a hozzájáruláson alapuló, a visszavonás előtti adatkezelés jogszerűségét. A hozzájárulás visszavonását ugyanolyan egyszerű módon kell lehetővé tenni, mint annak megadását.

Hozzájárulásra, mint jogalapra, a munkahelyi adatkezelések esetében csak kivételesen lehet hivatkozni a munkáltató és a munkavállaló között fennálló függelmi jelleg miatt.

A Szikszó Város Önkormányzata adatkezeléseihez kapcsolódóan a hozzájárulás alapú adatkezelések esetén a GDPR Reg Adatkezelési rendszerben is generálhat szerkeszthető hozzájáruló nyilatkozatot, mely tartalmazza a kiválasztott adatkezelésekre vonatkozóan az érintettek tájékoztatására szolgáló valamennyi adatot, információt.

1.8. Az érintett jogai

A Rendeletnek és az Infotv-nek megfelelően az érintettek az alábbi főbb jogokat gyakorolhatják:

1. **Előzetes tájékoztatáshoz való jog:** Az érintett magánszemély bármikor jogosult arra, hogy az adatkezeléssel összefüggő tényekről és információkról érthető, tömör tájékoztatást kapjon, ez a joga az adatkezelés megkezdését megelőzően is fennáll.
2. **A hozzáférésjoga:** Az érintett jogosult arra, hogy az adatkezelőtől tömör, közérthető visszajelzést kapjon arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e, és ha ilyen adatkezelés folyamatban van, jogosult arra, hogy a személyes adatokhoz és a Rendeletben felsorolt információkhoz hozzáférést kapjon.
3. **A helyesbítéshez való jog:** Az érintett jogosult arra, hogy kérésére az adatkezelő indokolatlan késedelem nélkül helyesbítse a rá vonatkozó pontatlan személyes adatokat. Figyelembe véve az adatkezelés célját, az érintett jogosult arra, hogy kérje a téves, hibás, hiányos személyes adatok – egyebek mellett kiegészítő nyilatkozat útján történő – módosítását, kiegészítését.
4. **A törléshez való jog:** Az érintett jogosult arra, hogy kérésére az adatkezelő indokolatlan késedelem nélkül törölje a rá vonatkozó személyes adatokat, az adatkezelő pedig köteles arra, hogy az érintettre vonatkozó személyes adatokat indokolatlan késedelem nélkül törölje meghatározott feltételek esetén (ha annak nincs jogi akadálya). Az érintettnek ez a joga különösen a hozzájárulása alapján kezelt személyes adataihoz kapcsolódóan áll fent, más jogalapok fennállta, így többek között a jogi kötelezettség teljesítése alapján kezelt adatok esetén pedig kifejezetten korlátozott ez a joga, illetve nem áll fent.
5. **Az elfeledtetéshez való jog:** Ha az adatkezelő nyilvánosságra hozta a személyes adatot, és azt törölni köteles, az elérhető technológia és a megvalósítás költségeinek figyelembevételével megteszi az észszerűen elvárható lépéseket – ideértve technikai intézkedéseket – annak érdekében, hogy tájékoztassa az adatokat kezelő adatkezelőket, hogy az érintett kérelmezte tőlük a szóban forgó személyes adatokra mutató linkek vagy e személyes adatok másolatának, illetve másodpéldányának törlését.

6. **Az adatkezelés korlátozásához való jog:** Az érintett jogosult arra, hogy kérésére az adatkezelő korlátozza az adatkezelést, ha az alábbi feltételek valamelyike teljesül:
- az érintett vitatja a személyes adatok pontosságát, ez esetben a korlátozás arra az időtartamra vonatkozik, amely lehetővé teszi, hogy az adatkezelő ellenőrizze a személyes adatok pontosságát,
 - az adatkezelés jogellenes, és az érintett ellenzi az adatok törlését, és e helyett kéri azok felhasználásának korlátozását,
 - az adatkezelőnek már nincs szüksége a személyes adatokra adatkezelés céljából, de az érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez, vagy védelméhez,
 - az érintett tiltakozott az adatkezelés ellen; ez esetben a korlátozás arra az időtartamra vonatkozik, amíg megállapításra nem kerül, hogy az adatkezelő jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben.
7. **A személyes adatok helyesbítéséhez vagy törléséhez, illetve az adatkezelés korlátozásához kapcsolódó értesítési kötelezettség:** Az adatkezelő minden olyan címzettet tájékoztat minden helyesbítésről, törlésről vagy adatkezelés-korlátozásról, akikkel a személyes adatot közölték. Kivétel: nem várható el ezen kötelezettség teljesítése, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényelne.
8. **Az adathordozhatósághoz való jog:** Az érintett jogosult arra, hogy a rá vonatkozó, általa egy adatkezelő rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja és jogosult arra, hogy ezeket az adatokat egy másik adatkezelőnek továbbítsa anélkül, hogy ezt akadályozná az az adatkezelő, amelynek a személyes adatokat a rendelkezésére bocsátotta.
9. **A tiltakozáshoz való jog:** Az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból bármikor tiltakozzon személyes adatainak a kezelése ellen (ideértve a profilalkotást is):
- ha az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához, illetve az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges (tiltakozás esetén a személyes adatok nem kezelhetők tovább, kivéve, ha az adatkezelő bizonyítja, hogy az adatkezelést olyan kényszerítő erejű jogos okok indokolják, amelyek elsőbbséget élveznek az érintett érdekeivel, jogaival és szabadságaival szemben, vagy amelyek jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódnak).
 - közvetlen üzletszerzés esetén: ha az érintett tiltakozik a személyes adatok közvetlen üzletszerzés érdekében történő kezelése ellen, akkor a személyes adatok a továbbiakban e célból nem kezelhetők.
10. **Automatizált döntéshozatal egyedi ügyekben, beleértve a profilalkotást:** Az érintett jogosult arra, hogy ne terjedjen ki rá az olyan, kizárólag automatizált adatkezelésen – ideértve a profilalkotást is – alapuló döntés hatálya, amely rá nézve joghatással járna vagy őt jelentős mértékben érintené (kivéve ha az adatkezelés az érintett és az adatkezelő közötti szerződés megkötése vagy teljesítése érdekében szükséges, vagy meghozatalát az adatkezelőre alkalmazandó olyan uniós vagy tagállami jog teszi lehetővé, amely az érintett jogainak és szabadságainak, valamint jogos érdekeinek védelmét szolgáló megfelelő intézkedéseket is megállapít, vagy az érintett kifejezett hozzájárulásán alapul).
11. **Az érintett tájékoztatása az adatvédelmi incidensről:** Adatkezelőnek indokolatlan késedelem nélkül tájékoztatnia kell az érintettet – ismertetve vele az Adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit, valamint az adatvédelmi incidensből eredő,

valószínűsíthető következményeket –, ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár jogaira és szabadságaira nézve, kivéve ha:

- adatkezelő megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre, melyeket az incidens által érintett adatok tekintetében alkalmaztak (pl. a titkosítás, amely a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné tesz az adatokat),
- 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,
- a tájékoztatás aránytalan erőfeszítést tenne szükségessé - ilyen esetekben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, vagy olyan hasonló intézkedést kell hozni, amely biztosítja az érintettek hasonlóan hatékony tájékoztatását.

- 12. A felügyeleti hatóságnál történő panasztételhez való jog** (hatósághoz való fordulás joga): Az érintett magánszemély jogosult arra, hogy panaszt tegyen egy felügyeleti hatóságnál – különösen a szokásos tartózkodási helye, a munkahelye vagy a feltételezett jogsértés helye szerinti tagállamban –, ha az érintett megítélése szerint a rá vonatkozó személyes adatok kezelése megsérti az uniós adatvédelmi rendeletet.
- 13. A felügyeleti hatósággal szembeni hatékony bírósági jogorvoslathoz való jog:** Minden természetes és jogi személy jogosult a hatékony bírósági jogorvoslatra a felügyeleti hatóság rá vonatkozó, jogilag kötelező erejű döntésével szemben. Ez a jog akkor is fennáll, ha a felügyeleti hatóság nem foglalkozik a panasszal, vagy három hónapon belül nem tájékoztatja az érintettet a benyújtott panasszal kapcsolatos eljárási fejleményekről vagy annak eredményéről.
- 14. Az adatkezelővel vagy az adatfeldolgozóval szembeni hatékony bírósági jogorvoslathoz való jog:** Minden érintett hatékony bírósági jogorvoslatra jogosult, ha megítélése szerint a személyes adatainak az uniós rendeletnek nem megfelelő kezelése következtében megsértették a jogait. Az bírósági illetékességi szabályok szerinti Törvényszék jogosult az eljárásra.
- 15. A személyes adatokkal összefüggő jogok érvényesítése az érintett halálát követően:** Az Infotv. szerint az érintett halálát követő öt éven belül a Rendelet hatálya alá tartozó adatkezelési műveletek esetén az elhatalt életében megillető jogokat az érintett által arra ügyintézési rendelkezéssel, illetve közokiratban vagy teljes bizonyító erőjű magánokiratban foglalt, az adatkezelőnél tett nyilatkozattal - ha az érintett egy adatkezelőnél több nyilatkozatot tett, a későbbi időpontban tett nyilatkozattal - meghatalmazott személy jogosult érvényesíteni. Ha az érintett nem tett megfelelő jognyilatkozatot, a Ptk. szerinti közeli hozzátartozója annak hiányában is jogosult az elhatalt életében megillető jogokat érvényesíteni az érintett halálát követő öt éven belül. Az érintett jogainak érvényesítésére az a közeli hozzátartozó jogosult, aki ezen jogosultságát elsőként gyakorolja.

1.9. Felelősségi körök, Szervezet vezetőjének feladatai

A Szikszó Város Önkormányzata vezetője (továbbiakban vezető) felelős azért, hogy az általa vezetett Szervezet az adatkezelési, adatfeldolgozási tevékenységét úgy végezze, hogy megfeleljen a Rendeletnek, amely szabályozza a természetes személyeknek a személyes adatok kezelése tekintetében történő védelmét és az ilyen adatok szabad áramlását, és biztosítja az érintettek számára a jogi garanciákat. Felelős azért, hogy az adatkezelési tevékenységek során betartsa a személyes adatok kezelésére vonatkozó elveket, és képes e megfelelések igazolására („elszámoltathatóság”).

Felelős azért, hogy:

- A személyes adatoknak bármilyen jellegű kezelése tekintetében az adatkezeléssel kapcsolatos hatásköröket és felelősségét egyértelműen meghatározza, szabályozza.
- Megfelelő és hatékony intézkedéseket hajtson végre, valamint képes legyen igazolni azt, hogy az adatkezelési tevékenységek a Rendeletnek megfelelnek, és az alkalmazott intézkedések hatékonysága is a Rendelet által előírt szintű. Az intézkedéseket az adatkezelés jellegének, hatókörének, körülményeinek és céljainak, valamint a természetes személyek jogait és szabadságait érintő kockázatnak a figyelembevételével kell meghozni.
- Megteremtse a szervezet informatikai rendszereinek és a benne kezelt adatoknak a biztonságát, meghatározza és biztosítsa a szervezet informatikai biztonsági követelményrendszerét és környezetét, az elektronikus információs rendszereivel kapcsolatba kerülő személyek felé támasztott követelményeket, elvárásokat, kötelezettségeket és a felelősséget.
- Olyan adatfeldolgozókat vegyen igénybe, amelyek megfelelő garanciákat nyújtanak – különösen a szakértelem, a megbízhatóság és az erőforrások tekintetében – arra vonatkozóan, hogy az a rendelet követelményeinek teljesülését biztosító technikai és szervezési intézkedéseket végrehajtják, ideértve az adatkezelés biztonságát is.
- A Rendelet előírásai szerint szükség szerint képviselőt vagy kapcsolattartót jelöljön ki, aki az adatkezeléssel összefüggő ügyekben (pl. incidens bejelentése, stb.) kapcsolattartó pontként szolgál az érintettekkel, felügyeleti hatósággal (NAIH), valamint adott esetben bármely egyéb kérdésben konzultációt folytathat vele. Megvizsgálja, köteles-e Adatvédelmi tisztviselőt kinevezni, vagy önként sor kerül-e kinevezésére. Felelőssége a kapcsolattartóval kapcsolatos bármilyen módosulást, változást azonnal, késedelem nélkül az érintettek tudomására hozni (tájékoztató, bejelentés, stb.).

1.10. Adatvédelmi tisztviselő

A vezető nevezi ki az Adatvédelmi tisztviselőt, akinek kinevezését, jogállását lásd a *2.1. Adatvédelmi tisztviselő kijelölése* fejezetnél.

1.11. Képzés

A vezető jóváhagyta a szükséges felkészültséget, kompetenciát valamennyi munkatársa, illetve a vele szerződéses jogviszonyban álló valamennyi magánszemély és szervezet/intézmény esetében, amelynek munkavállalói vagy alvállalkozói a szervezet által használt rendszerekhez, személyes adatokhoz, adatkezelési műveletekhez hozzáféréssel rendelkeznek, illetve akik részt vesznek a szervezetnél keletkezett, feldolgozott, tárolt, illetve továbbított személyes adatok kezelésében. Feladata, hogy biztosítsa az adatkezelési műveletekben résztvevő külső és belső munkatársak folyamatos tudatosság-növelését, hogy felkészültek legyenek a megfelelő oktatások, képzések, gyakorlat alapján.

Felelőssége, hogy folyamatosan kiértékelje az elvégzett tevékenységek eredményességét, biztosítsa, hogy a munkatársak tudatában legyenek az adatkezelési/adatfeldolgozási tevékenységében betöltött szerepüknek és annak fontosságának.

Feladata, hogy felmérje a képzési szükségleteket és megszervezze az adatkezeléssel kapcsolatos külső és belső oktatásokat, képzéseket, és ezekről a megfelelő feljegyzéseket (pl. Oktatási tematika, Oktatási napló, stb.) megőrizze. Szükség szerinti gyakorisággal, legalább évente egyszer képzést szervez vagy online képzést tart, ahol ismertetésre kerül a Rendeletet és jelen Adatvédelmi és adatbiztonsági szabályzat előírásai. Cél a munkatársak és a közreműködők tudatosság-növelése és folyamatos továbbképzése, a szervezeti adatvédelmi szabályok fontosságának előtérbe helyezése, bemutatása.

Felelősége a személyes adatokba állandó jelleggel vagy rendszeresen betekintő személyzetnek nyújtandó megfelelő személyre szóló adatvédelmi továbbképzés szervezése, valamint közös képzési és csereprogramok (pl. felügyeleti hatóságok között, valamint adott esetben harmadik országok felügyeleti hatóságaival vagy nemzetközi szervezetekkel) támogatása.

2. A szervezet adatvédelmi feladatai

2.1. Adatvédelmi tisztviselő kijelölése

Kötelező a kinevezés, mivel az adatkezelést közhatalmi szerv vagy egyéb, közfeladatot ellátó szerv végzi.

Az Adatvédelmi tisztviselőt a szakmai rátermettsége és különösen az adatvédelmi jog és gyakorlat szakértői szintű ismerete, valamint a Rendeletben az Adatvédelmi tisztviselő feladatai között felsorolt feladatok ellátására való alkalmassága alapján kell megbízni.

Közhatalmi szerv vagy egyéb, közfeladatot ellátó szerv közös Adatvédelmi tisztviselőt jelölhet ki több ilyen szerv számára, az adott szervek szervezeti felépítésének és méretének figyelembevételével.

A Szervezet támogatása az Adatvédelmi tisztviselő munkájához:

- biztosítja, hogy az Adatvédelmi tisztviselő a személyes adatok védelmével kapcsolatos összes ügybe megfelelő módon és időben bekapcsolódjon,
- biztosítja azokat a forrásokat, amelyek e feladatok végrehajtásához, a személyes adatokhoz és az adatkezelési műveletekhez való hozzáféréshez, valamint az Adatvédelmi tisztviselő szakértői szintű ismereteinek fenntartásához szükségesek,
- biztosítja, hogy az Adatvédelmi tisztviselő a feladatai ellátásával kapcsolatban utasításokat senkitől ne fogadjon el, őt a feladatai ellátásával összefüggésben nem bocsáthatja el, és szankcióval nem sújthatja,
- az Adatvédelmi tisztviselőt minden személyes adattal kapcsolatos, személyes adatot érintő kérdésbe bevonja,
- önállóan vagy közös Adatvédelmi tisztviselő által képviselt szervezetekre vonatkozóan együttesen biztosít az Adatvédelmi tisztviselő hatósági bejelentése, kommunikációja és az érintettekkel való közvetlen és folyamatos kapcsolattartás érdekében egy – lehetőleg kizárólag erre a célra szolgáló – e-mail-címet, ehhez a tisztviselő számára hozzáférést (pl. adatvedelem@domain.hu).

Az Adatvédelmi tisztviselő jogállása:

- az Adatvédelmi tisztviselő közvetlenül a Szervezet vezetőjének tartozik felelősséggel,
- az érintettek a személyes adataik kezeléséhez és a Rendelet szerinti jogaik gyakorlásához kapcsolódó valamennyi kérdésben az Adatvédelmi tisztviselőhöz fordulhatnak,
- feladatai teljesítésével kapcsolatban uniós vagy tagállami jogban meghatározott titoktartási kötelezettség vagy az adatok bizalmas kezelésére vonatkozó kötelezettség köti,
- az Adatvédelmi tisztviselő más feladatokat is elláthat, a vezetés biztosítja, hogy e feladatokból ne fakadjon összeférhetetlenség.

Az Adatvédelmi tisztviselő legalább a következő feladatokat látja el:

- tájékoztat és szakmai tanácsot ad a vezetőség, továbbá az adatkezelést végző alkalmazottak, közreműködők részére a Rendelet, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezések szerinti kötelezettségeikkel kapcsolatban,

- ellenőrzi a Rendeletnek, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezéseknek, továbbá a Szervezet 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,
- kérésre szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, valamint nyomon követi a hatásvizsgálat elvégzését,
- együttműködik a felügyeleti hatósággal,
- az adatkezeléssel összefüggő ügyekben – ideértve az előzetes konzultációt is – kapcsolattartó pontként szolgál a felügyeleti hatóság felé, valamint adott esetben bármely egyéb kérdésben konzultációt folytat vele.

Az Adatvédelmi tisztviselő jogviszonyának fennállása alatt és azt követően is köteles titokként megőrizni a vonatkozó tevékenységével kapcsolatban tudomására jutott azon személyes adatot, minősített adatot, törvény által titoknak minősített adatot, illetve minden olyan adatot, tényt vagy körülményt, amelyet az őt alkalmazó adatkezelő vagy adatfeldolgozó törvény előírása alapján nem köteles nyilvánosságra hozni.

A Rendelet 37. cikk (7) bekezdése szerint az adatkezelőnek vagy adatfeldolgozónak az általa kijelölt Adatvédelmi tisztviselő elérhetőségét közzé kell tennie és erről tájékoztatnia kell az illetékes felügyeleti hatóságot. Az Infotv. 25/L. § (4) bekezdése szerint az adatkezelő, illetve az adatfeldolgozó tájékoztatja a Hatóságot az Adatvédelmi tisztviselő nevéről, postai és elektronikus levélcíméről, ezen adatok változásáról, valamint ezen adatokat nyilvánosságra hozza. A Nemzeti Adatvédelmi és Információszabadság Hatóság az adatkezelők, illetve adatfeldolgozók számára külön erre a célra létrehozott elektronikus felületen is lehetővé teszi az Adatvédelmi tisztviselő bejelentését.

A Szikszó Város Önkormányzata az Adatvédelmi tisztviselő kijelölést, azzal kapcsolatos információkat (pl. jogállás), a tisztviselő adatait a GDPR Reg Adatkezelési rendszerben dokumentálja, tartja nyilván.

Az aktuálisan szereplő adatok feltüntetésre kerülnek az adatkezelési tájékoztatókban és valamennyi dokumentumban.

2.2. Adatkezelési, adatfeldolgozói tevékenységek nyilvántartása

A Szikszó Város Önkormányzata egyes adatkezelések tekintetében:

- önálló adatkezelőnek minősül (a személyes adatok kezelésének céljait és eszközeit önállóan határozza meg)
- közös adatkezelőnek minősülhet (a személyes adatok kezelésének céljait és eszközeit másokkal együtt határozza meg)
- adatfeldolgozónak minősülhet (valamely adatkezelő nevében személyes adatokat kezel)

A Szervezet, mint adatkezelő és adatfeldolgozó a felelősségébe tartozóan végzett adatkezelési, adatfeldolgozási tevékenységekről nyilvántartást vezet, mivel a Rendelet alapján nem mentesül a nyilvántartás-vezetési kötelezettség alól, valamint így tudja teljesíteni az elszámoltathatóság elvét, mely szerint az adatkezelő felelős a személyes adatok kezelésére vonatkozó elveknek (lásd 1.4 fejezet) való megfelelésért, továbbá képesnek kell lennie e megfelelés igazolására. A nyilvántartásokat a felügyeleti hatóság részére rendelkezésre bocsátja.

Az Adatkezelési nyilvántartás a következő információkat tartalmazza:

- az adatkezelő neve és elérhetősége, valamint – ha van ilyen – a közös adatkezelőnek, az adatkezelő képviselőjének és az Adatvédelmi tisztviselőnek a neve és elérhetősége;
- az adatkezelés céljai;
- az érintettek kategóriáinak, valamint a személyes adatok kategóriáinak ismertetése;
- olyan címzettek kategóriái, akikkel a személyes adatokat közlik vagy közölni fogják, ideértve a harmadik országbeli címzetteket vagy nemzetközi szervezeteket;
- 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 továbbítás esetében a megfelelő garanciák leírása;
- ha lehetséges, a különböző adatkategóriák törlésére előírt határidők;
- ha lehetséges, a technikai és szervezési intézkedések általános leírása.

Ha van olyan adatkezelés, ahol a Szervezet adatfeldolgozónak minősül, akkor szükséges az adatfeldolgozói nyilvántartás, mely a következő információkat tartalmazza:

- 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;
- az egyes adatkezelők nevében végzett adatkezelési tevékenységek kategóriái;
- adott esetben a személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítása, beleértve a harmadik ország vagy a nemzetközi szervezet azonosítását, valamint továbbítás esetében a megfelelő garanciák leírása;
- ha lehetséges, a technikai és szervezési intézkedések általános leírása.

A Szikszó Város Önkormányzata az adatkezelési, adatfeldolgozói tevékenységeket a GDPR Reg Adatkezelési rendszerben tartja nyilván. Az adatkezelő és az adatfeldolgozó nevében végzett adatkezelési tevékenységek nyilvántartásai a Rendelet követelményei szerinti, aktuális adattartalommal tartalmazza rendszerben szereplő, egyedileg rögzített adatkezeléseket.

2.3. Átlátható tájékoztatás, kommunikáció és az érintett jogainak gyakorlására vonatkozó intézkedések

A Szervezet megfelelő intézkedéseket hozott annak érdekében, hogy az érintett (bármely információ alapján azonosított vagy azonosítható természetes személy) részére a személyes adatok kezelésére vonatkozó valamennyi tájékoztatást tömör, átlátható, érthető és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazva nyújtsa, különösen a gyermekeknek címzett bármely információ esetében. Az információkat írásban vagy más módon – ideértve adott esetben az elektronikus utat is – kell megadni. Az érintett kérésére szóbeli tájékoztatás is adható, feltéve, hogy más módon igazolásra kerül az érintett személyazonossága. Az érintetti kérelmek kezelését lásd a 2.4 fejezetben.

2.3.1. Tájékoztatás és a személyes adatokhoz való hozzáférés joga

Ha az érintettre vonatkozó személyes adatokat az érintettől gyűjtik, akkor az átlátható tájékoztatás és a személyes adatokhoz való hozzáférés joga érdekében az adatkezelő az adatok megszerzésének időpontjában, illetve az adatkezelés megkezdését megelőzően Adatkezelési tájékoztatókban vagy egyéb módon az érintettek rendelkezésére bocsátja a Rendeletben előírt információkat:

- a munkáltatói szerepkörben, a munkaviszonyhoz vagy egyéb foglalkoztatásra irányuló jogviszonyhoz kapcsolódóan folytatott adatkezelési műveletekre vonatkozó adatkezelésekről írásban tájékoztatja a munkavállalókat, a tudomásulvétel feljegyzését megőrzi;
- a tevékenységével kapcsolatos adatkezelésekről (pl. hatósági eljárások során végzett adatkezelésekről) az ügyfeleket egy vagy több adatkezelési tájékoztatóban tájékoztatja, a tájékoztató minden olyan helyen rendelkezésre áll elektronikus vagy nyomtatott formában, ahol szükséges az érintettek tájékoztatása;
- további adatkezelések, főként az információs társadalommal összefüggő szolgáltatások (elektronikus úton, távollevők részére nyújtott szolgáltatás) esetén az adatkezelési tájékoztatót az érintettek előzetes tájékoztatására elektronikusan, internetes honlapon, digitális formában, bárki számára, személyazonosítás nélkül, korlátozástól mentesen hozzáférhetővé teszi. A közfeladatot ellátó szervek az elektronikus közzétételt saját vagy társulásaik által közösen működtetett, illetve a felügyeletüket, szakmai irányításukat vagy működésükkel kapcsolatos koordinációt ellátó szervek által fenntartott, erre a célra létrehozott központi honlapon való közzététellel biztosíthatják;
- ha a személyes adatokon a gyűjtésük céljától eltérő célból további adatkezelést kíván végezni, a további adatkezelést megelőzően tájékoztatja az érintettet erről az eltérő célról és minden releváns kiegészítő információról;
- az érintett rendelkezésére bocsátandó információkra vonatkozó szabályok nem alkalmazandóak, ha és amilyen mértékben az érintett már rendelkezik az információkkal.

Az Adatkezelési tájékoztató tartalmazza az alábbiakat:

- az adatkezelőnek és – ha van ilyen – az adatkezelő képviselőjének a kiléte és elérhetőségei,
- az Adatvédelmi tisztviselő elérhetőségei,
- a személyes adatok tervezett kezelésének célja,
- az adatkezelés jogalapja,
- a személyes adat szolgáltatása jogszabályn vagy szerződéses kötelezettségen alapul vagy szerződés kötésének előfeltétele-e, valamint hogy az érintett köteles-e a személyes adatokat megadni, továbbá hogy milyen lehetséges következményekkel járhat az adatszolgáltatás elmaradása,
- ha az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, akkor az adatkezelő, vagy harmadik fél jogos érdekei,
- a személyes adatok tárolásának időtartama, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjai,
- adott esetben a személyes adatok címzettjei, illetve a címzettek kategóriái, ha van ilyen,
- adott esetben annak ténye, hogy az adatkezelő harmadik országba vagy nemzetközi szervezet részére kívánja továbbítani a személyes adatokat,
- automatizált döntéshozatal ténye, ideértve a profilalkotást is, valamint legalább ezekben az esetekben az alkalmazott logikára és arra vonatkozóan érthető információk, hogy az ilyen adatkezelés milyen jelentőséggel, és az érintettre nézve milyen várható következményekkel bír,

- tájékoztatás az érintett azon jogáról, hogy kérelmezheti az adatkezelőtől a rá vonatkozó személyes adatokhoz való hozzáférést, azok helyesbitését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen, valamint az érintett adathordozhatóságához való joga,
- az érintett hozzájárulásán alapuló adatkezelés esetén a hozzájárulás bármely időpontban történő visszavonásához való jog, amely nem érinti a visszavonás előtt a hozzájárulás alapján végrehajtott adatkezelés jogszerűségét,
- a felügyeleti hatósághoz címzett panasz benyújtásának joga.

Ha az érintettre vonatkozó személyes adatokat nem az érintettől gyűjtik: az adatkezelőnek az adatkezelési tájékoztatás során fentiekén kívül rendelkezésre bocsátani a személyes adatok forrását és adott esetben azt, hogy az adatok nyilvánosan hozzáférhető forrásokból származnak-e.

A tájékoztatást a személyes adatok kezelésének konkrét körülményeit tekintetbe véve, a személyes adatok megszerzésétől számított észszerű határidőn, de legkésőbb egy hónapon belül, ha a személyes adatokat az érintettel való kapcsolattartás céljára használják, legalább az érintettel való első kapcsolatfelvétel alkalmával, vagy ha várhatóan más címmel is közlik az adatokat, legkésőbb a személyes adatok első alkalommal való közlésekor kell megadni.

Az érintett rendelkezésére bocsátandó információkra vonatkozó szabályok nem alkalmazandóak, ha és amilyen mértékben az érintett már rendelkezik az információkkal, az információk rendelkezésre bocsátása lehetetlennek bizonyul vagy aránytalanul nagy erőfeszítést igényelne, az adat megszerzését vagy közlését kifejezetten előírja az adatkezelőre alkalmazandó uniós vagy tagállami jog, vagy a személyes adatoknak valamely uniós vagy tagállami jogban előírt szakmai titoktartási kötelezettség alapján bizalmasnak kell maradnia.

A Szikszó Város Önkormányzata az érintettek tájékoztatóit a Rendelet követelményei szerinti adattartalommal GDPR Reg Adatkezelési rendszerben készíti el az előzetesen egyedileg összeállított, folyamatosan aktualizált adatkezelések adataival.

A szerkeszthető adatkezelési tájékoztatók kategóriánként generálhatók, abból a célból, hogy személyre szabott tájékoztatóval tudja tájékoztatni az érintetteket (készülnek munkavállalói, ügyfelekkel kapcsolatos, és szakmai, valamint egyedileg létrehozott kategóriával kapcsolatos adatkezelési tájékoztatók, ha vannak).

Az Ügyfelekkel kapcsolatos aktuális adatkezelési tájékoztató honlapon is publikálásra kerül, ennek megkönnyítésére lehetséges a tájékoztatót tartalmazó weboldal domain nevéhez egyedi un. API kód generálása. A weboldalt üzemeltető által elvégzett egyszeri kódbeillesztést követően automatikusan megjelenik a weboldalon az ügyfelekkel kapcsolatos aktuális adatkezelési tájékoztató.

2.3.2. Az érintett hozzáférési joga

Az adatkezelés teljes tartama alatt az érintett jogosult a megadott elérhetőségeken tájékoztatást és hozzáférést kérni az adatkezelő által kezelt személyes adatokról, valamint az adatkezelés jellemzőiről:

- az adatkezelés céljáról,
- az érintett személyes adatok kategóriáiról,
- a címzettekről vagy címzettek kategóriáiról, akikkel, illetve amelyekkel a személyes adatokat közölték vagy közölni fogják, különösen a harmadik országbeli címzetteket, nemzetközi szervezeteket,

- a személyes adatok tárolásának tervezett időtartamáról, vagy az időtartam meghatározásának szempontjairól,
- az érintett személyes adatai kezelésével kapcsolatos helyesbítési, törlési, korlátozási vagy tiltakozási jogairól,
- a valamely felügyeleti hatósághoz címzett panasz benyújtásának jogáról,
- ha az adatokat nem az érintettől gyűjtötték, a forrásukra vonatkozó minden elérhető információról,
- az automatizált döntéshozatal tényéről, ideértve a profilalkotást is, az alkalmazott logikára és arra vonatkozó érthető információkról, hogy az ilyen adatkezelés milyen jelentőséggel bír, és az érintettre nézve milyen várható következményekkel jár,
- a valamely felügyeleti hatósághoz címzett panasz benyújtásának jogáról,
- illetve a Tájékoztatás és a személyes adatokhoz való hozzáférés joga alapján a 2.3.1 pontban felsorolt valamennyi információról (ami az adatkezelési tájékoztató kötelező tartalmi eleme).

A személyes adatoknak harmadik országba vagy nemzetközi szervezet részére történő továbbítása esetén az érintett jogosult arra, hogy tájékoztatást kapjon a továbbításra vonatkozóan az adattovábbítás megfelelő garanciáiról.

Az adatkezelő az érintett kérésére az adatkezelés tárgyát képező személyes adatok másolatát rendelkezésére bocsátja. Lásd a 2.4. *Érintetti kérelmek kezelése* fejezetet.

2.3.3. Az érintett helyesbítéshez való joga

Az érintett jogosult kérelmezni személyes adatainak helyesbítését. Amennyiben adatai megváltoztak, vagy nem pontosak, akkor kérelmére - a személyes adatok kezelésének ideje alatt - bármikor módosítja azokat az adatkezelő.

2.3.4. A törléshez, elfeledtetéshez való jog

Az Érintett hozzájárulásán alapuló adatkezelés esetén az érintett bármikor visszavonhatja hozzájárulását és kérheti, hogy adatait törölje az adatkezelő, amennyiben az adatkezelésnek nincs további jogalapja. A visszavonás nem érinti a visszavonás előtt a hozzájárulás alapján végrehajtott adatkezelés jogszerűségét.

Az érintett az alábbi indokok valamelyikének fennállása esetén jogosult arra, hogy kérésére az adatkezelő indokolatlan késedelem nélkül törölje a rá vonatkozó személyes adatokat:

- személyes adatokra már nincs szükség abból a célból, amelyből azokat gyűjtötték vagy más módon kezelték;
- az érintett visszavonja az adatkezelés alapját képező hozzájárulását, és az adatkezelésnek nincs más jogalapja;
- az érintett tiltakozik az adatkezelés ellen, és nincs elsőbbséget élvező jogszerű ok az adatkezelésre;
- a személyes adatokat jogellenesen kezelték;
- a személyes adatokat az adatkezelőre alkalmazandó uniós vagy tagállami jogban előírt jogi kötelezettség teljesítéséhez törölni kell;
- a személyes adatok gyűjtésére információs társadalommal összefüggő szolgáltatások kínálásával kapcsolatosan került sor.

Az adatok törlési kérelme elutasítható, ha az adatkezelés szükséges:

- a véleménynyilvánítás szabadságához és a tájékozódáshoz való jog gyakorlása céljából;

- 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;
- közérdekből vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlása keretében végzett feladat végrehajtása céljából;
- a népegészségügy területét érintő közérdekből;
- a közérdekű archiválás, tudományos és történelmi kutatási vagy statisztikai célból, ha a törlési jog valószínűsíthetően lehetetlenné tenné vagy komolyan veszélyeztetné ezt az adatkezelést.

Ha az adatkezelő nyilvánosságra hozta a személyes adatot, és azt törölni köteles, az elérhető technológia és a megvalósítás költségeinek figyelembevételével megteszi az észszerűen elvárható lépéseket – ideértve technikai intézkedéseket – annak érdekében, hogy tájékoztassa az adatokat kezelő adatkezelőket, hogy az érintett kérelmezte tőlük a szóban forgó személyes adatokra mutató linkek vagy e személyes adatok másolatának, illetve másodpéldányának törlését.

2.3.5. Az adatkezelés korlátozásához való jog

Az adatkezelő korlátozza a személyes adatok kezelését, ha ezt kéri az érintett. Az érintett a következő esetekben kérheti az adatai korlátozását:

- amennyiben vitatja adatai pontosságát, ez esetben a korlátozás arra az időtartamra vonatkozik, amely lehetővé teszi, hogy az adatkezelő ellenőrizze a személyes adatok pontosságát;
- amennyiben az adatkezelés jogellenes és az érintett ellenzi adatainak törlését és ehelyett kéri azok korlátozását;
- az adatkezelőnek már nincs szüksége a személyes adatokra az adatkezelés céljából, de az érintett igényli azokat jogi igényének előterjesztéséhez, érvényesítéséhez vagy védelméhez;
- az érintett tiltakozik az adatkezelés ellen, ez esetben a korlátozás arra az időtartamra vonatkozik, amíg megállapításra nem kerül, hogy az adatkezelő jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben.

Ha az adatkezelés korlátozás alá esik, a személyes adatokat a tárolás kivételével csak az érintett hozzájárulásával, valamint jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez, vagy más természetes vagy jogi személy jogainak védelme érdekében, vagy az Unió, illetve valamely tagállam fontos közérdekből lehet kezelni. Az érintettet az adatkezelés korlátozásának feloldásáról előzetesen tájékoztatni kell.

A személyes adatok kezelésének korlátozására alkalmazott módszerek közé tartozhat többek között a szóban forgó személyes adatoknak egy másik adatkezelő rendszerbe történő ideiglenes áthelyezése vagy a felhasználók számára való hozzáférhetőségük megszüntetése, illetve egy honlapról az ott közzétett adatok ideiglenes eltávolítása. Az adatkezelés korlátozását az automatizált nyilvántartási rendszerekben alapvetően technikai eszközökkel kell biztosítani, oly módon, hogy a személyes adatokon további adatkezelési műveleteket ne végezzenek el és azokat ne lehessen megváltoztatni. Azt a tényt, hogy a személyes adatok kezelése korlátozott, egyértelműen jelezni kell a rendszerben.

2.3.6. A személyes adatok helyesbítéséhez vagy törléséhez, illetve az adatkezelés korlátozásához kapcsolódó értesítési kötelezettség

Minden olyan címzettet tájékoztatni kell a helyesbítésről, törlésről vagy adatkezelés-korlátozásról, akivel, illetve amellyel a személyes adat közlésre került, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel. Az érintettet kérésére az adatkezelő tájékoztatja e címzettekről.

2.3.7. Az adathordozhatósághoz való jog

Ha az adatkezelés hozzájáruláson alapul, vagy szerződés teljesítéséhez szükséges és az adatkezelés automatizált módon történik, az érintettek adatait gépi nyilvántartással kezelik, az érintett jogosult arra, hogy a rá vonatkozó, az általa az adatkezelő rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja, ezeket egy másik adatkezelőnek továbbítsa. Jogosult arra, hogy – ha ez technikailag megvalósítható – kérje a személyes adatok adatkezelők közötti közvetlen továbbítását. Az adatok hordozhatóságához való jog nem érinti hátrányosan mások jogait és szabadságait, illetve nem alkalmazandó abban az esetben, ha az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítványai gyakorlásának keretében végzett feladat végrehajtásához szükséges.

2.3.8. A tiltakozáshoz való jog

Az érintett jogosult saját helyzetével kapcsolatos okból bármikor tiltakozni személyes adatai kezelése ellen, ha adatkezelő az adatokat saját vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges vagy közérdekű/adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges jogalpból kezeli, ideértve az említett rendelkezéseken alapuló profilalkotást is. A tiltakozási jogára legkésőbb az érintettel való első kapcsolatfelvétel során kifejezetten fel kell hívni a figyelmét, és az erre vonatkozó tájékoztatást egyértelműen, minden más információtól elkülönítve kell megjeleníteni. A tiltakozáshoz való jogot az információs társadalommal összefüggő szolgáltatások igénybevételéhez kapcsolódóan műszaki előírásokon alapuló automatizált eszközökkel is gyakorolhatja.

Tiltakozás esetén a személyes adatot nem kezelheti tovább az adatkezelő, kivéve, ha bizonyítja, hogy az adatkezelést olyan kényszerítő erejű jogos okok indokolják, amelyek elsőbbséget élveznek az érintett érdekeivel, jogaival és szabadságával szemben, vagy amelyek jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódnak. Tudományos és történelmi kutatási vagy statisztikai célú adatkezelés esetén az érintett nem élhet tiltakozási jogával, ha az adatkezelésre közérdekű okból végzett feladat végrehajtása érdekében van szükség.

Tiltakozás közvetlen üzletszerzés esetén: Az érintett tiltakozhat, ha a személyes adatok kezelése közvetlen üzletszerzés érdekében történik, ideértve a profilalkotást is, amennyiben az a közvetlen üzletszerzéshez kapcsolódik. Ha tiltakozik a személyes adatok közvetlen üzletszerzés érdekében történő kezelése ellen, akkor a személyes adatok a továbbiakban e célból nem kezelhetők.

2.3.9. Automatizált döntéshozatal egyedi ügyekben, profilalkotás

Az érintett jogosult arra, hogy ne terjedjen ki rá az olyan, kizárólag automatizált adatkezelésen – ideértve a profilalkotást is – alapuló döntés hatálya, amely rá nézve joghatással járna vagy őt hasonlóképpen jelentős mértékben érintené.

Nem alkalmazható a fenti jogosultság, ha az automatizált döntéshozatal:

- az érintett és az adatkezelő közötti szerződés megkötése vagy teljesítése érdekében szükséges,

- meghozatalát az adatkezelőre alkalmazandó olyan uniós vagy tagállami jog teszi lehetővé, amely az érintett jogainak és szabadságainak, valamint jogos érdekeinek védelmét szolgáló megfelelő intézkedéseket is megállapít,
- az érintett kifejezett hozzájárulásán alapul.

A szerződés megkötése vagy teljesítése érdekében szükséges vagy az érintett kifejezett hozzájárulásán alapuló adatkezelések esetén megfelelő intézkedéseket kell tenni az érintett jogainak, szabadságainak és jogos érdekeinek védelme érdekében, ideértve az érintettnek legalább azt a jogát, hogy az adatkezelő részéről emberi beavatkozást kérjen, álláspontját kifejezze, és a döntéssel szemben kifogást nyújtson be.

Az automatizált döntéshozatal nem alapulhat a személyes adatoknak különleges kategóriáin, kivéve ha az érintett kifejezett hozzájárulását adta vagy az adatkezelés jelentős közérdek miatt szükséges, uniós jog vagy tagállami jog alapján, és az érintett jogainak, szabadságainak és jogos érdekeinek védelme érdekében megfelelő intézkedések megtételére került sor.

2.3.10. A személyes adatokkal összefüggő jogok érvényesítése az érintett halálát követően

Az Infotv. szerint az érintett halálát követő öt éven belül a Rendelet hatálya alá tartozó adatkezelési műveletek esetén az elhaltat életében megillető egyes jogokat (a hozzáféréshez és a törléshez való jogokat) az érintett által arra ügyintézési rendelkezéssel, illetve közokiratban vagy teljes bizonyító erejű magánokiratban foglalt, az adatkezelőnél tett nyilatkozattal - ha az érintett egy adatkezelőnél több nyilatkozatot tett, a későbbi időpontban tett nyilatkozattal - meghatalmazott személy jogosult érvényesíteni.

Ha az érintett nem tett megfelelő jognyilatkozatot, a Ptk. szerinti közeli hozzátartozója annak hiányában is jogosult a Rendelet hatálya alá tartozó adatkezelési műveletek esetén a helyesbítéshez és tiltakozáshoz való jogot, valamint - ha az adatkezelés már az érintett életében is jogellenes volt vagy az adatkezelés célja az érintett halálával megszűnt – a Rendelet hatálya alá tartozó adatkezelési műveletek esetén a Rendeletben az adatkezelés korlátozásához, törléshez való jogot, mint az elhaltat életében megillető jogokat érvényesíteni az érintett halálát követő öt éven belül. Az érintett jogainak e bekezdés szerinti érvényesítésére az a közeli hozzátartozó jogosult, aki ezen jogosultságát elsőként gyakorolja.

Az érintett jogait érvényesítő személyt e jogok érvényesítése - így különösen az adatkezelővel szembeni, valamint a Hatóság, illetve bíróság előtti eljárás - során az e törvény által az érintett részére megállapított jogok illetik meg és kötelezettségek terhelik.

Kérelemre tájékoztatni kell az érintett Ptk. szerinti közeli hozzátartozóját megtett intézkedésekről, kivéve, ha azt az érintett nyilatkozatában megtiltotta.

2.4. Az érintetti kérelmek kezelése

Az érintett magánszemélynek, személy azonosítása mellett lehetősége van bármely általa választott módon kérelmet benyújtani személyesen, postai úton, elektronikus levélben, meghatalmazott útján, illetve egyéb módon. A tájékoztatást az érintett által kért módon kell megadni, elektronikus úton benyújtott kérelem esetén lehetőség szerint elektronikus úton kell megadni.

A Szikszó Város Önkormányzata megfelelő intézkedéseket hozott annak érdekében, hogy az érintett részére a személyes adatok kezelésére vonatkozó valamennyi tájékoztatást tömör, átlátható, érthető és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazva nyújtsa. Az információkat írásban vagy más módon – ideértve adott esetben az elektronikus utat is – kell megadni. Az érintett kérésére szóbeli tájékoztatás is adható, feltéve, hogy más módon igazolásra kerül az érintett személyazonossága.

Indokolatlan késedelem nélkül, de legfeljebb a kérelem beérkezésétől számított egy hónapon belül tájékoztatja az érintettet jogai gyakorlására irányuló kérelmében foglaltak teljesítéséről, a kérelem nyomán hozott intézkedésekről. Szükség esetén, figyelembe véve a kérelem összetettségét és a kérelmek számát, ez a határidő további két hónappal meghosszabbítható.

Ha nem tesz intézkedéseket az érintett kérelme nyomán, késedelem nélkül, de legkésőbb a kérelem beérkezésétől számított egy hónapon belül tájékoztatja az érintettet az intézkedés elmaradásának okairól, a késedelem okainak megjelölésével, valamint arról, hogy az érintett panaszt nyújthat be valamely felügyeleti hatóságnál, és élhet bírósági jogorvoslati jogával.

Amennyiben úgy ítéli meg, hogy az érintett magánszemély kérelmének teljesítésére nincs lehetőség, úgy a kérelem elutasításáról és a Rendelet szerinti jogorvoslati jogokról tájékoztatja a kérelmezőt.

Az érintetti kérelmek kezelése, teljesítése a Szervezet vezetője vagy az általa kijelölt személy feladata. Indokolt esetben be kell vonni az Adatvédelmi tisztviselőt vagy jogi szakértőt.

A Szervezet biztosítja a jogot az érintettek számára, hogy a felügyeleti hatósághoz történő panasztétellel párhuzamosan bírósági jogorvoslatot is igényeljenek, amennyiben megítélésük szerint valamely adatkezelő vagy adatfeldolgozó a személyes adataiknak kezelése során megsértette adatvédelemre vonatkozó jogait. Az érintett által kezdeményezett bírósági eljárás során nem az érintettnek kell bizonyítania adatvédelemmel kapcsolatos jogai megsértését, hanem az adatkezelő vagy adatfeldolgozó köteles bizonyítani azt, hogy az érintett ezen jogai nem sérültek.

Adatkezelő a kérelem benyújtásakor jogosult és köteles ellenőrizni a kérelmező személyazonosságát az adatok bizalmasága és jogi kötelezettségek teljesítése érdekében. Az azonosítás lehetőség szerint az adatmegadás, adatszerzés módjához kapcsolódik. Érintetti kérelem alapján történő eljárás esetén az adatigénylő személyazonosító adatai csak annyiban kezelhetők, amennyiben az az igény teljesítéséhez - beleértve az esetleges költségek megfizetését is - elengedhetetlenül szükséges.

A Szervezet az érintetti tájékoztatások, kérelmek elbírálása és teljesítése során tevékenységéért költséget, díjazást nem számol fel, de az egyértelműen megalapozatlan vagy ismételt, túlzó jellegű kérelmek esetén, figyelemmel a kért információ vagy tájékoztatás nyújtásával vagy a kért intézkedés meghozatalával járó adminisztratív költségekre, jogosult észszerű összegű díj felszámítására, illetve megtagadhatja a kérelem alapján történő intézkedést. A kérelem egyértelműen megalapozatlan vagy túlzó jellegének bizonyítása az adatkezelőt terheli. Erre vonatkozó rendelkezéshiányában a kérelem teljesítéséért megállapítható költségek a 301/2016. (IX. 30.) Korm. rendeletben foglalt költségek figyelembevételével kerülnek megállításra.

A Szikszó Város Önkormányzata az érintettek kérelmeit a GDPR Reg Adatkezelési rendszerben is nyilvántarthatja, elkészítheti a szükséges dokumentumokat. A rendszer támogatja az adatkezelőt az érintett magánszemélyek GPRG Rendelet 15–22. cikk szerinti jogainak a gyakorlásával kapcsolatos feladatokban. A generált szerkeszthető dokumentum tartalmazza az adatkezelő és az érintett kérelmező főbb adatait, a kiválasztott adatkezelés(ek) leírását és tájékoztatást a panasz benyújtáshoz vagy bírósági jogorvoslatához való jogról.

2.5. Az adatkezelés biztonsága, technikai és szervezési intézkedések végrehajtása

A Szikszó Város Önkormányzata, mint adatkezelő és adatfeldolgozó a felelősségébe tartozóan végzett adatkezelési, adatfeldolgozási tevékenységekkel kapcsolatban a tudomány és technológia állása és a megvalósítás költségei, továbbá 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 érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja.

A Szervezet vezetője felelős azért, hogy figyelembe véve a szervezet méretét, a folyamatok bonyolultságát és kölcsönhatását, a személyzet kompetenciáját, valamint a vonatkozó törvényeket, előírásokat, elvárásokat, meghatározza informatikai- és adatbiztonsági követelményrendszerét és környezetét.

Az adatkezelés biztonsága érdekében meghatározott technikai, szervezési intézkedéseket a 4.fejezet tartalmazza részletesen.

A Szikszó Város Önkormányzata a GDPR Reg Adatkezelési rendszerben is rögzítheti az adatkezelésekkel kapcsolatos technikai, szervezési intézkedéseket, az aktuális adatokkal a nyilvántartások nyomtathatóak.

2.6. Az adatvédelmi incidensek

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.

A Szikszó Város Önkormányzata, mint adatkezelő kötelessége, hogy amint tudomására jut egy adatvédelmi incidens (pl. felmerül a gyanú, hogy Szervezet számítógépes biztonsági incidens áldozatává vált, vagy éppen ennek folyamata alatt van) azt indokolatlan késedelem nélkül kivizsgálja, és szükség esetén bejelentsé (ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott) az illetékes felügyeleti hatóságnál (NAIH).

A Szervezet, mint adatkezelő/adatfeldolgozó felelőssége megbizonyosodni arról, hogy az összes megfelelő technológiai védelmi és szervezési intézkedés végrehajtásra került-e, egyrészt az adatvédelmi incidens haladéktalan megállapítása, másrészt a felügyeleti hatóságnak történő bejelentés és az érintett sürgős értesítése érdekében. Azt, hogy az értesítésre indokolatlan késedelem nélkül került-e sor, különösen az adatvédelmi incidens jellegére és súlyosságára, valamint annak az érintettre gyakorolt következményeire, illetve hátrányos hatásaira figyelemmel kell megállapítani.

Ha a Szervezet adatfeldolgozónak minősül egyes adatkezelések tekintetében, a Rendeletben foglalt kötelezettségének megfelelően az arról való tudomásulvételt követően indokolatlan késedelem nélkül bejelenti az adatkezelőnek.

2.6.1. Incidensek belső nyilvántartása

Amennyiben az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve, akkor a Szervezet saját nyilvántartásába veszi.

2.6.2. Incidens NAIH bejelentése

Az érintettre nézve valószínűsíthető kockázat esetén bejelenti az incidenst a NAIH erre a célra szolgáló elektronikus Adatvédelmi Incidensbejelentő Rendszer felületén, vagy ennek hiányában postai úton. Ha nem lehetséges az információkat egyidejűleg közölni, akkor azok indokolatlan késedelem nélkül részletekben is közölhetők. Ha a bejelentés 72 órán belül nem történt meg, akkor a bejelentésben meg kell jelölni a késedelem okát.

A bejelentést a NAIH által elvárt adattartalommal kell teljesíteni. A szervezeti adatokon, az Adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó kapcsolattartó nevén és elérhetőségén kívül tartalmaznia kell:

- az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát;
- az adatvédelmi incidensből eredő, valószínűsíthető következményeket;
- adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

2.6.3. Érintettek tájékoztatása az Incidensről

Adatkezelő feladata, hogy az érintettet indokolatlan késedelem nélkül tájékoztassa abban az esetben, ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár jogaira és szabadságaikra nézve, annak érdekében, hogy megtehessek a szükséges óvintézkedéseket. Az érintett részére adott tájékoztatásban a szervezeti adatokon, az Adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó kapcsolattartó nevén és elérhetőségén kívül világosan és közérthetően ismertetni kell az adatvédelmi incidens jellegét, az incidensből eredő, valószínűsíthető következményeket, az incidens orvoslására tett vagy tervezett intézkedéseket, adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

Az érintettek tájékoztatása mellőzhető ha:

- adatkezelő megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre, melyeket az incidens által érintett adatok tekintetében alkalmaztak (pl. a titkosítás, amely a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné tesz az adatokat),
- 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,
- a tájékoztatás aránytalan erőfeszítést tenne szükségessé - ilyen esetekben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, vagy olyan hasonló intézkedést kell hozni, amely biztosítja az érintettek hasonlóan hatékony tájékoztatását.

2.6.4. Adatvédelmi incidensek kezelése

Minden vélt vagy valós adatvédelmi incidensről késedelem nélkül, a megadott kapcsolattartási csatornák valamelyikén értesíteni kell az Adatvédelmi tisztviselőt vagy hiányában a kapcsolattartásra kijelölt felelőst vagy a Szervezet vezetőjét.

Az adatvédelmi incidenst észlelő személy köteles a tapasztalt jelenséget minden rendelkezésére álló eszközzel dokumentálni, azokat haladéktalanul az Adatvédelmi tisztviselő vagy hiányában a kijelölt felelős vagy vezető rendelkezésére bocsátani (pl. feljegyzés, képernyőkép, fotó, hibaüzenet, stb.).

Az adatvédelmi incidens jelentésére vonatkozó kötelezettség valamennyi munkaviszony vagy foglalkoztatásra irányuló jogviszony alapján foglalkoztatottra, közreműködő munkatársra, valamint szerződéses, vagy más módon kapcsolatba kerülő természetes vagy jogi személyekre, gazdasági társaságokra, intézményekre vonatkozik, a velük kötött megállapodás, vagy titoktartási nyilatkozatok szerint.

A Szervezet vezetője által kijelölt felelős teendői:

- a körülmények ismeretében felméri a kockázatokat és meghatározza a kategóriát (nincs/van/magas kockázat),

- szükség esetén eseti szakértői csoportot hoz létre az incidens körülményeinek kivizsgálására, akik segítik a munkáját,
- értesíti a szervezet vezetőjét,
- meghatározza az értesítendőök körét,
- amennyiben az adatbiztonsági incidens IT biztonsági esemény is egyben, intézkedést tesz annak megszüntetésére, vagy az esemény jellegéből adódóan annak izolálására (az izolálást azonnal meg kell kezdeni, az érintett felek bevonásával), az Ibtv. hatálya alá tartozó szervezetek esetén késedelem nélkül értesíteni kell az elektronikus információs rendszerek biztonságáért felelős személyt is,
- meghatározza az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát,
- felméri az adatvédelmi incidensből eredő, valószínűsíthető következményeket,
- meghatározza az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket,
- az adatvédelmi incidensről, valamint annak életútjáról jegyzőkönyvet/nyilvántartást készít,
- indokolatlan késedelem nélkül bejelenti az illetékes Nemzeti Adatvédelmi és Információszabadság Hatóságnak, kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve,
- indokolatlan késedelem nélkül tájékoztatja az érintetteket az adatvédelmi incidensről, ha az valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve,
- amennyiben nem volt lehetséges az adatvédelmi incidenssel kapcsolatos információkat egyidejűleg közölni illetékes hatósággal, akkor azokat további indokolatlan késedelem nélkül később részletekben közli a hatósággal,
- irányítja a károk helyreállítását és a jogszerű működés visszaállítását,
- lezárja az adatvédelmi incidens kezelésének folyamatát és a kapcsolódó dokumentumokat,
- ellenőrzi a Rendeletnek, valamint a Szervezet személyes adatok védelmével kapcsolatos belső szabályainak való megfelelést, valamint áttekinti az érintettek jogainak védelmét szolgáló korrekciós intézkedéseket biztosító mechanizmusokat, és az incidensek kezelésére vonatkozó intézkedéseket, és azok eredményességét. Az ellenőrzés tapasztalatai szükség szerint beépülhetnek az adatvédelmi szabályozásba, illetve részét képezhetik a munkatársak képzésének, tovább képzésének.

A Szikszó Város Önkormányzata az adatvédelmi incidensek nyilvántartására, a hatósági adatszolgáltatásra a GDPR Reg Adatkezelési rendszert alkalmazza, melyben a NAIH által elvárt minimális adattartalommal rögzíthetők az incidensekkel kapcsolatos adatok, azokból a hatóság számára benyújtható dokumentum generálható.

2.7. Érdekmérlegelés

Az adatkezelő – ideértve azt az adatkezelőt is, akivel a személyes adatokat közölhetik – vagy valamely harmadik fél jogos érdeke jogalapot teremthet az adatkezelésre, feltéve hogy az érintett érdekei, alapvető jogai és szabadságai nem élveznek elsőbbséget, figyelembe véve az adatkezelővel való kapcsolata alapján az érintett észszerű elvárásait. Jogos érdekről lehet szó, amikor releváns és megfelelő kapcsolat áll fenn az

érintett és az adatkezelő között, például olyan esetekben, amikor az érintett az adatkezelő ügyfele vagy annak alkalmazásában áll, vagy személyes adatok közvetlen üzletszerzési célú kezelése esetén.

Közhatalmi szervek esetén a jogalkotó feladata, hogy jogszabályban határozza meg, a kötelező adatkezelések részleteit. A jogos érdekre hivatkozást, mint jogalapot nem lehet alkalmazni a közhatalmi szervek által feladataik ellátása során végzett adatkezelésre.

Az adatkezelés akkor lehet jogszerű az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges jogalapra hivatkozással, ha adatkezelő a jogos érdek fennállásának megállapításához elvégezte az érdekmérlegelési tesztet, annak eredménye az, hogy az adatkezelés szükséges és arányos, adatkezelő jogos érdeke megállapítható.

Az érdekmérlegelés során megállapításra kerül, hogy az érintett magánszemély személyhez fűződő jogait az adatkezelés milyen mértékben korlátozza, az érintett érdekei és alapvető jogai elsőbbséget élveznek-e az adatkezelő érdekével szemben, figyelembe véve az adatkezelővel való kapcsolata alapján az észszerű elvárásait.

A jogos érdek fennállásának megállapításához körültekintően meg kell vizsgálni többek között azt, hogy az érintett a személyes adatok gyűjtésének időpontjában és azzal összefüggésben számíthat-e észszerűen arra, hogy adatkezelésre az adott célból kerülhet sor. Az érintett érdekei és alapvető jogai elsőbbséget élvezhetnek az adatkezelő érdekével szemben, ha a személyes adatokat olyan körülmények között kezelik, amelyek középtette az érintettek nem számítanak további adatkezelésre.

Az adatkezelő más jogalapon történő adatkezelés mellett is elvégezheti az érdekmérlegelési tesztet az érintettek magánszférájának arányos korlátozása érdekében.

2.8. Adatközlés, adattovábbítás, nyilvánosságra hozatal

Adattovábbítás az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele.

A Szervezet az érintettek személyes adatainak továbbítását az egyes adatkezelések tekintetében, kizárólag jelen szabályzatban meghatározottak alapján és feltételek szerint valósítja meg.

Harmadik fél részére adatot csak akkor továbbíthat, ha az alábbi feltételek közül legalább egy megvalósul:

- az érintett ehhez az adatkezelés során előzetesen hozzájárulását adta és ha az adatkezelés feltételei minden egyes adatra nézve teljesülnek;
- a törvény az adattovábbítást megengedi és az adatkezelés feltételei minden egyes személyes adatra nézve teljesülnek;
- az adatkezelőre vonatkozó jogi kötelezettség teljesítése céljából szükséges;
- az adatkezelő vagy harmadik személy jogos érdekének érvényesítése céljából szükséges, és ezen érdek érvényesítése a személyes adatok védelméhez fűződő jog korlátozásával arányban áll;
- a nemzetbiztonság, a honvédelem és a közbiztonság védelme, a bűncselekmények üldözése céljából az arra hatáskörrel rendelkező nemzetbiztonsági szerveknek, nyomozó hatóságoknak, bíróságoknak, valamint egyéb bírósági és nyomozó szervek jogszerű megkeresése esetén átadhatók az adattovábbítási kérelemben megjelölt adatok tekintetében.

Személyes adatot csak akkor hozhat nyilvánosságra, ha erre megfelelő jogalappal rendelkezik. A személyes adatokon is alapuló, de anonimizált statisztikai adatok szabadon nyilvánosságra hozhatók.

2.8.1. Adattovábbítás harmadik országokba

A Szervezet jelenleg nem továbbít személyes adatokat harmadik országokba vagy nemzetközi szervezetek részére. A Vezetőfelelős azért, amennyiben személyes adatoknak harmadik országba vagy nemzetközi szervezet részére történő továbbítására kerülne sor, az érintett jogosult arra, hogy tájékoztatást kapjon a továbbításra vonatkozóan a megfelelő garanciákról. A személyes adatoknak az Unióból harmadik országbeli adatkezelőknek, adatfeldolgozóknak, egyéb címzetteknek vagy nemzetközi szervezetek részére történő továbbítása esetén nem sérülhet a természetes személyeknek az Unióban a Rendelettel biztosított védelem szintje, és annak fenn kell maradnia az ilyen személyes adatoknak az adott harmadik országból vagy nemzetközi szervezettől ezt követően ugyanazon vagy másik harmadik országbeli adatkezelőnek, adatfeldolgozónak vagy nemzetközi szervezetnek történő újbóli továbbítása esetén is.

A harmadik országokba és a nemzetközi szervezetekhez való továbbítás csak a Rendelet teljes betartása mellett hajtható végre. A továbbításra akkor kerülhet csak sor, ha az adatkezelő vagy az adatfeldolgozó – e rendelet egyéb rendelkezéseire is figyelemmel – teljesíti az harmadik országok vagy nemzetközi szervezeteknek történő adattovábbításra vonatkozó, e rendeletben meghatározott feltételeket.

Az Ibtv. hatálya alá tartozó szervezeteknek az Ibtv. 3. § (2) - (5) bekezdése bizonyos esetekben ad lehetőséget, hogy egyes elektronikus információs rendszereit Magyarország területén kívül üzemeltesse, illetve azokban külföldön végezzenek adatkezelést. Az adatkezelés kezdetét legalább 90 nappal megelőzően írásbeli kérelmet kell benyújtani a Hatóságnak (nem szükséges a hatóság engedélye, ha a külföldi adatkezelést vagy üzemeltetést nemzetközi szerződés írja elő).

A kérelemhez csatolni kell:

- az EGT tagállamaiban történő adatkezelés indokát,
- az EGT tagállamaiban kezelt adatok és adatbázisok leírását,
- azt, hogy az adatkezelő rendszer, valamint üzemeltetője nevesített-e, és az adatkezelés jogszabályi megfeleléséért felelős személy neve, beosztása, elérhetősége ismert-e,
- az adatkezelő rendszer technikai és technológiai leírását, ideértve a hardver- és szoftverkomponenseket is,
- az adatkezelő rendszer információbiztonságának ismertetését, a rendszerhez kapcsolódó, továbbá az üzemeltetőre vonatkozó belső szabályozásokat és utasításokat,
- a kötelezően lefolytatandó biztonsági rendszerfelülvizsgálat eredményét,
- a magyar információvédelmi szabályok megtartásáról szóló üzemeltetői nyilatkozatot,
- azt, hogy az üzemeltetés helyszínén illetékes hatóságok jogosultak-e a kezelt adatokba betekinteni.

2.9. Adatfeldolgozás, adatfeldolgozói garancianyújtás

A Szervezet a felelősségébe tartozóan végzett adatkezelési, adatfeldolgozási tevékenységekről nyilvántartást vezet a 2.2. fejezet szerint.

A Szervezet, mint adatkezelő:

Ha a Szervezet az adatkezelő (a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt határozza meg), de bizonyos adatkezelési tevékenységekhez adatfeldolgozó szolgáltatásait is igénybe veszi, kizárólag olyan közreműködőt (adatfeldolgozót) vehet igénybe, aki megfelelő garanciákat nyújt az adatkezelés Rendelet követelményeinek való megfelelését és az érintettek jogainak védelmét biztosító, megfelelő technikai és szervezési intézkedések végrehajtására vonatkozóan.

Az adatfeldolgozó tevékenységet végző közreműködőket az Adatkezelési nyilvántartásban kell nyilvántartani.

Az adatfeldolgozó szerződéseknek célszerűen az alábbiakat kell tartalmaznia:

- az adatkezelő és az adatfeldolgozó személyét, elérhetőségét, ha az adatfeldolgozó rendelkezik Adatvédelmi tisztviselővel, annak elérhetőségét,
- az adatfeldolgozás jellegét, célját, időtartamát,
- az adatfeldolgozással érintett adatalanyok kategóriáit, a személyes adatok típusát, körét, mennyiségét,
- az adatfeldolgozó jogainak és kötelezettségeinek meghatározását, különösen annak rögzítését, hogy az adatfeldolgozó az adatkezelő kifejezett írásos utasításai alapján végezhet adatkezelési műveleteket, továbbá az esetlegesen bekövetkező adatvédelmi incidensek esetén követendő szabályok meghatározását,
- az elvégzett technikai műveletek megnevezését, módját,
- a feldolgozott személyes adatok további sorsát,
- annak rögzítését, hogy az adatfeldolgozó további adatfeldolgozót vehet-e igénybe,
- az adatkezelőt és az adatfeldolgozót terhelő technikai és szervezési intézkedések meghatározását, ezek igazolását az adatfeldolgozó részéről,
- az adatfeldolgozó azon alkalmazottai titoktartására vonatkozó rendelkezéseket, akik az adatfeldolgozásban részt vesznek,
- annak szabályozását, hogy az adatfeldolgozó milyen módon, eljárási rendet követve nyújt segítséget az érintettek jogait érintő kérelmek megválaszolásában,
- az adatkezelő ellenőrzési jogkörének biztosítását,
- az adatkezelő utasításadási rendjének meghatározását, beleértve az adatfeldolgozó azon kötelezettségét, hogy tájékoztassa az adatkezelőt, ha az adatkezelő által adott utasítás GDPR vagy egyéb vonatkozó jogszabályba ütközik,
- minden olyan információ adatkezelő rendelkezésre bocsátását, amely meghatározott kötelezettségek teljesítésének igazolásához szükséges, amely lehetővé teszi és elősegíti az adatkezelő által vagy az általa megbízott más ellenőr által végzett auditokat, beleértve a helyszíni vizsgálatokat is,
- az adatkezelési szolgáltatás nyújtásának befejezését követő eljárást (pl. az adatkezelő döntése alapján minden személyes adatot töröl, vagy visszajuttat, és törli a meglévő másolatokat, kivéve, ha az uniós vagy a tagállami jog a személyes adatok tárolását írja elő).

A Szervezet mint adatfeldolgozó:

A Szikszó Város Önkormányzata adatfeldolgozó tevékenysége során (ha van) az adatokat kizárólag az adatkezelő utasításának megfelelően kezeli, kivéve, ha az ettől való eltérésre uniós vagy tagállami jog kötelezi.

Afeladatok ellátásához megfelelő ismerettel és gyakorlattal rendelkező személyeket vesz igénybe. Biztosítja, hogy az érintett személyes adatokhoz való hozzáférésre feljogosított személyek – ha jogszabályon alapuló megfelelő titoktartási kötelezettség hatálya alatt egyébként nem állnak – az általuk megismert személyes adatok vonatkozásában titoktartási kötelezettséget vállaljanak.

A tudomány és technológia állása és a megvalósítás költségei, továbbá 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 érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja.

Az adatkezelő előzetesen írásban tett eseti vagy általános felhatalmazása nélkül további adatfeldolgozót nem vesz igénybe. Az általános írásbeli felhatalmazás esetén tájékoztatja az adatkezelőt minden olyan tervezett változásról, amely további adatfeldolgozók igénybevételét vagy azok cseréjét érinti, ezzel biztosítva lehetőséget az adatkezelőnek arra, hogy ezekkel a változtatásokkal szemben kifogást emeljen.

Ha bizonyos, az adatkezelő nevében végzett konkrét adatkezelési tevékenységekhez további adatfeldolgozó szolgáltatásait is igénybe veszi, uniós vagy tagállami jog alapján létrejött szerződés vagy más jogi aktus útján erre a további adatfeldolgozóra is ugyanazok az adatvédelmi kötelezettségeket kell telepíteni, mint amelyek az adatkezelő és az adatfeldolgozó között létrejött szerződésben vagy egyéb jogi aktusban szerepelnek.

A további adatfeldolgozónak megfelelő garanciákat kell nyújtania a megfelelő technikai és szervezési intézkedések végrehajtására, biztosítania kell, hogy az adatkezelés megfeleljen a Rendelet követelményeinek. Ha a további adatfeldolgozó nem teljesíti adatvédelmi kötelezettségeit, az őt megbízó adatfeldolgozó teljes felelősséggel tartozik az adatkezelő felé a további adatfeldolgozó kötelezettségeinek a teljesítéséért.

Az adatkezelés jellegének figyelembevételével megfelelő technikai és szervezési intézkedésekkel a lehetséges mértékben segíti az adatkezelőt abban, hogy teljesíteni tudja kötelezettségét az érintett jogainak gyakorlásához kapcsolódó kérelmek megválaszolása tekintetében.

Segíti az adatkezelőt kötelezettségei teljesítésében, figyelembe véve az adatkezelés jellegét és a rendelkezésére álló információkat.

Az adatkezelő rendelkezésére bocsát minden olyan információt, amely kötelezettségei teljesítésének igazolásához szükséges, lehetővé teszi és elősegíti az adatkezelő által vagy az általa megbízott más ellenőr által végzett auditokat, beleértve a helyszíni vizsgálatokat is.

Az adatkezelés biztonsága érdekében meghatározott technikai, szervezési intézkedéseket az adatkezelővel kötött megállapodás tartalmazza, illetve a 4. fejezetben szerepelnek az adatkezelés során betartott intézkedések.

2.10. Kötelező adatkezelések felülvizsgálata

Az Infotv. 5.§ (3)-(5)bekezdése alapján az alábbi kötelező adatkezelések(Rendelet 6. cikk (1) c), e)pont) esetén a kezelendő adatok fajtáit, az adatkezelés célját és feltételeit, az adatok megismerhetőségét, az adatkezelő személyét, valamint az adatkezelés időtartamát vagy szükségessége időszakos felülvizsgálatát az adatkezelést elrendelő törvény, illetve önkormányzati rendelet határozza meg.

Ha a kötelező adatkezelés időtartamát vagy szükségessége időszakos felülvizsgálatát törvény, helyi önkormányzat rendelete vagy az Európai Unió kötelező jogi aktusa nem határozza meg, az adatkezelő az adatkezelés megkezdésétől legalább háromévente felülvizsgálja, hogy az általa, illetve a megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által kezelt személyes adat kezelése az adatkezelés céljának megvalósulásához szükséges-e.

Ezen felülvizsgálat körülményeit és eredményét az adatkezelő dokumentálja, e dokumentációt a felülvizsgálat elvégzését követő tíz évig megőrzi és azt a Nemzeti Adatvédelmi és Információszabadság Hatóság kérésére rendelkezésére bocsátja.

A Szikszó Város Önkormányzata a GDPR Reg Adatkezelési rendszerben végzi el és dokumentálja az adatkezelések felülvizsgálatát az egyes adatkezelésekre beállított felülvizsgálati gyakorisággal.

2.11. Adatvédelmi hatásvizsgálat

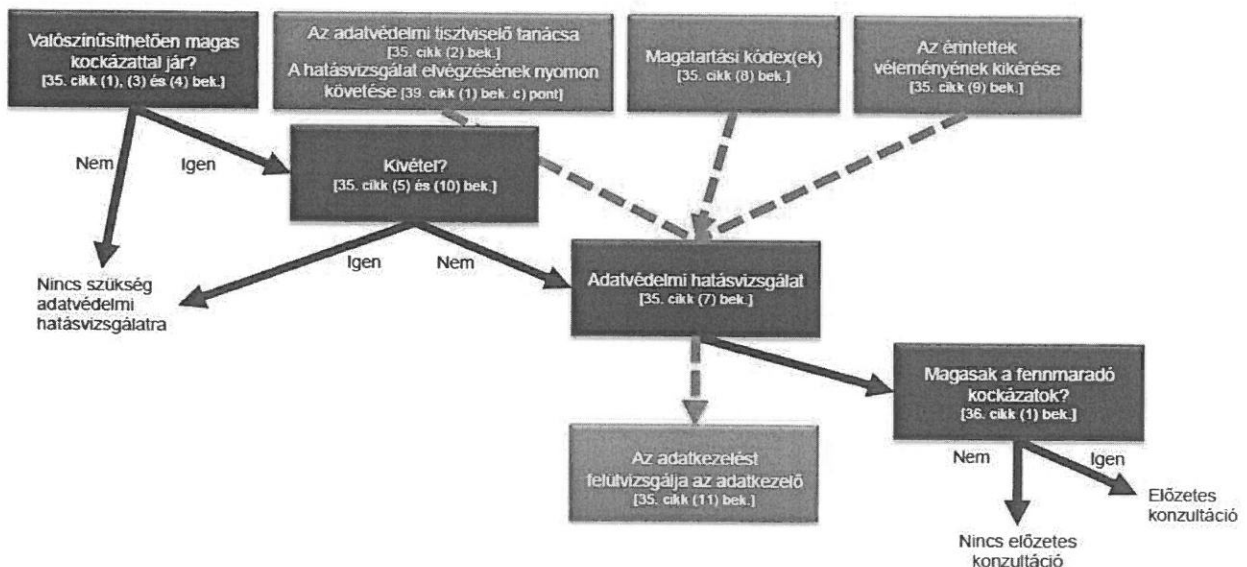
A természetes személyek jogaira és szabadságaira nézve magas kockázattal járó esetekben az adatkezelő – annak érdekében, hogy az adatkezelés jellegét, hatókörét, körülményeit és céljait, valamint a kockázat forrásait figyelembe véve felmérje a magas kockázat különös valószínűségét és súlyosságát – az adatkezelés előtt adatvédelmi hatásvizsgálatot végez arra vonatkozóan, hogy a tervezett adatkezelési műveletek a személyes adatok védelmét hogyan érintik. Ez magában foglalja különösen az említett kockázat mérséklését, a személyes adatok védelmét, a Rendeletnek való megfelelés bizonyítását célzó tervezett intézkedéseket, garanciákat és mechanizmusokat.

Az adatvédelmi hatásvizsgálatot az alábbi esetekben kell elvégezni:

- természetes személyekre vonatkozó egyes személyes jellemzők olyan módszeres és kiterjedt értékelése, amely automatizált adatkezelésen – ideértve a profilalkotást is – alapul, és amelyre a természetes személy tekintetében joghatással bíró vagy a természetes személyt hasonlóképpen jelentős mértékben érintő döntések épülnek,
- különleges adatok nagy számban történő kezelése,
- nyilvános helyek nagymértékű, módszeres megfigyelése,
- minden olyan adatkezelés tekintetében, amelyek valószínűsíthetően magas kockázattal járnak az érintettek nézve.

A hatásvizsgálat kiterjed legalább:

- a tervezett adatkezelési műveletek módszeres leírására és az adatkezelés céljainak ismertetésére (beleértve adott esetben az adatkezelő által érvényesíteni kívánt jogos érdeket);
- az adatkezelés céljaira figyelemmel az adatkezelési műveletek szükségességi és arányossági vizsgálatára;
- az érintett jogait és szabadságait érintő kockázatok vizsgálatára; és
- a kockázatok kezelését célzó intézkedések bemutatására (a személyes adatok védelmét, és a Rendelettel való összhang igazolását szolgáló, az érintettek és más személyek jogait és jogos érdekeit figyelembe vevő garanciákra, biztonsági intézkedésekre, mechanizmusokra.



Az adatvédelmi hatásvizsgálatot a kijelölt felelős(ök) végzi(k) el, szükség szerint be kell vonni az érintett vezetőket, felelősöket (pl. informatikai, informatikai biztonsággal foglalkozó felelősöket). Az Adatvédelmi tisztviselő szakmai tanácsát ki kell kérni, a döntés során figyelembe kell venni.

A 2018. május 25-e előtt megkezdett és hatásvizsgálat elvégzését igénylő adatkezelések esetén az Infotv. 75.§ (3) bekezdése alapján legkésőbb 2021. május 25-ig végre kell hajtani a vizsgálatot, illetve azonnal, amennyiben az adatkezelés körülményeiben lényeges változás következik be.

A Szervezet, mint adatkezelő szükség szerint, de legalább az adatkezelési műveletek által jelentett kockázat változása esetén ellenőrzést folytat le annak értékelése céljából, hogy a személyes adatok kezelése az adatvédelmi hatásvizsgálatnak megfelelően történik-e.

Nem szükséges elvégezni a hatásvizsgálatot azokra az adatkezelési műveletekre, melyek jogalapját uniós vagy az adatkezelőre alkalmazandó tagállami jog írja elő, és e jog a szóban forgó, e jogalap elfogadása során egy általános hatásvizsgálat részeként már végeztek adatvédelmi hatásvizsgálatot (kivéve ha a tagállamok az adatkezelési tevékenységet megelőzően ilyen hatásvizsgálat elvégzését szükségesnek tartják).

Olyan egymáshoz hasonló típusú adatkezelési műveletek, amelyek egymáshoz hasonló magas kockázatokat jelentenek, egyetlen hatásvizsgálat keretei között is értékelhetők.

A hatásvizsgálat szükségességének megállapítását dokumentálni kell, a vizsgálat során figyelembe kell venni a felügyeleti hatóság által összeállított adatkezelések jegyzékét.

A Szikszó Város Önkormányzata az egyes adatkezelésekre vonatkozóan az adatvédelmi hatásvizsgálat szükségességét, a természetes személyek jogaira és szabadságára nézve valószínűsíthető kockázatokat a GDPR Reg Adatkezelési rendszerben vizsgálja meg a NAIH által összeállított adatkezelési műveletek típusainak a jegyzéke alapján, az adatkezelő által figyelembe vett egyéb szempontok figyelembevételével.

A Szervezet a hatásvizsgálatok lefolytatásánál figyelembe veszi, hogy a kockázati tényezők azonosításában nagy szerepe lehet az érintettek érdekeinek mérlegelése során az érintettekkel való konzultációnak. Az érintetti vélemények kikérése, beépítése, dokumentálása javasolt, ennek hiányát indokolni kell.

Ha az adatvédelmi hatásvizsgálat megállapítja, hogy az adatkezelés az adatkezelő által a kockázat mérséklése céljából tett intézkedések hiányában valószínűsíthetően magas kockázattal jár, a személyes adatok kezelését megelőzően konzultáció szükséges a felügyeleti hatósággal.

A Szikszó Város Önkormányzata a hatásvizsgálatot igénylő egyes adatkezelésre vagy az egymáshoz hasonló típusú, hasonló magas kockázatú adatkezelési műveletek esetén azok csoportjára az adatvédelmi kockázatok felmérését és a megfelelő kockázatkezelést, az intézkedések végrehajtását a GDPR Reg Adatkezelési rendszerben is elvégezheti és dokumentálhatja.

3. Személyes adatok kezelése, nyilvántartása

3.1. Munkavállalók adatkezelései

A Szervezet minden munkavállalójának (mint érintett természetes személy) személyes adatainak kezeléséért a Szervezet vezetője a felelős, aki biztosítja, hogy a munkaviszonyhoz, kormányzati szolgálati jogviszonyhoz vagy egyéb foglalkoztatásra irányuló jogviszonyhoz (továbbiakban jogviszonyhoz)

kapcsolódóan folytatott adatkezelési műveletekre vonatkozóan, valamint az adatfeldolgozók részére átadott adatok kapcsán az adatfeldolgozókkal is betartatja a Rendelet előírásait és a munkahelyi adatkezelések alapvető követelményeit.

A munkavállaló személyiségi joga akkor korlátozható, ha a korlátozás a jogviszony rendeltetésével közvetlenül összefüggő okból feltétlenül szükséges és a cél elérésével arányos. A személyiségi jog korlátozásának módjáról, feltételeiről és várható tartamáról, továbbá szükségességét és arányosságát alátámasztó körülményekről a munkavállalót előzetesen írásban tájékoztatni kell. A munkáltatónak szükségességi-arányossági tesztet kell végeznie, amely alapján igazolja a személyiségi jog korlátozásának jogszerűségét és azt, hogy az adatkezelés nem indokolatlan beavatkozás a munkavállaló magánszférájába.

Az érintett személy számára a munkáltató feladata az adatkezelés megkezdése előtt egyértelmű és részletes tájékoztatást adni az adatai kezelésével kapcsolatos minden jelentős tényről.

A Szikszó Város Önkormányzata a munkavállalók adatkezelési tájékoztatóit a GDPR Reg Adatkezelési rendszerben készíti el az előzetesen egyedileg összeállított, folyamatosan aktualizált adatkezelések adataival a személyre szabott tájékoztatáshoz. A munkavállalói adatkezelési tájékoztatót tudomásulvétel igazolása céljából aláírattatja, archiválja vagy helyben szokásos és általában ismert módon közzéteszi.

A hozzájárulás alapján történő adatkezelés

A hozzájárulás egy vagy több célra jogalapon történő adatkezelés esetén az érintett munkavállaló írásbeli hozzájárulását adja személyes adatainak egy vagy több konkrét célból történő kezeléséhez. A jelenlegi joggyakorlat alapján munkaviszonyban a munkavállaló hozzájárulása az esetek döntő többségében a jogviszony függelmi jellege miatt nem lehet önkéntes, mert egyfajta egyensúlytalanság, hatalmi viszony áll fent a munkáltató javára. Hozzájárulásra, mint jogalapra, a munkahelyi adatkezelések esetében csak kivételesen lehet hivatkozni, alapvetően akkor, amikor egyértelmű, hogy az adatkezelés során feltétel nélküli „előnyöket” szerez a munkavállaló, és nem érheti őt semmilyen hátrány a hozzájárulás megtagadása esetén (ebben az esetben dokumentált előzetes tájékoztatás után egy tényleges szöveges, magyarázattal ellátott hozzájárulás aláírásával lehet bizonyítani a munkavállaló önkéntességét, megadva a lehetőséget a nemleges válaszra is). Egy hozzájárulás egy adatkezelési cél érdekében végzett adatkezeléshez való hozzájárulást jelenti. Több adatkezelési cél esetén több önkéntes, egyértelmű érintetti hozzájárulás szükséges.

Adatkezelés munkáltatói jogos érdek alapján, munkáltatói ellenőrzések

A Szikszó Város Önkormányzata, mint adatkezelőnek a munkavállalókkal kapcsolatosan, azoknak a fennálló jogviszonya alatt, illetve azt megelőzően és azt követően is fűződhet érdeke személyes adatok kezeléséhez. Adatkezelő vagy valamely harmadik fél jogos érdeke jogalapot teremthet az adatkezelésre, feltéve, hogy az érintett érdekei, alapvető jogai és szabadságai nem élveznek elsőbbséget, figyelembe véve az adatkezelővel való kapcsolata alapján az érintett észszerű elvárásait. Munkáltató a jogos érdek fennállásának megállapításához érdek mérlegelést végez, melynek során azt kívánja eldönteni, hogy az érintett magánszemély személyhez fűződő jogait az adatkezelés milyen mértékben korlátozza, az érintett érdekei és alapvető jogai elsőbbséget élveznek-e az adatkezelő érdekével szemben.

A Szikszó Város Önkormányzata a jogos érdeke fennállásának megállapításához szükséges érdek mérlegelést a GDPR Reg Adatkezelési rendszerben dokumentálja. Az Érdék mérlegelés – Jogos

érdek vizsgálata dokumentumot az elszámoltathatóság, bizonyíthatóság érdekében aláírva archiválja és megismerteti az érintettekkel.

A Szervezet vezetője, mint munkáltató felelős azért, hogy az adatkezelés célját minden esetben világosan és egyértelműen határozza meg, a szükségesség-arányosság elvének megfelelően, az alkalmazott eszköz alkalmas legyen a megfogalmazott adatkezelési cél elérésére, csak szükséges mértékű adatkezeléssel járjon, és ellenőrzés csak a munkavégzéssel összefüggésben történjen, és soha nem irányuljon a munkavállalók emberi méltóságának a sérelmére, így a munkavállalók megfélemlítésére, megalázására, zaklatására, zavarására. A munkavállaló magánszférája meg kell, hogy maradjon. A munkavállalókat a munkahelyen is megilleti a magánélethez való jog, amelyeknek tipikus színterei: ebédlő, öltöző, pihenő helyiség, mosdók.

A munkavállaló a munkáltató által a munkavégzéshez biztosított számítástechnikai eszközt – eltérő megállapodás, rendelkezés hiányában – kizárólag a jogviszony teljesítése érdekében használhatja, tilos a munkahelyi infrastruktúra magán használatára.

A munkavállaló a jogviszonnyal összefüggő magatartása körében ellenőrizhető, akár technikai eszköz alkalmazásával is. Munkáltató kötelezettsége, hogy munkáltatói rendelkezéseinek, egyéb szabályoknak, pl. az informatikai biztonságra vonatkozó követelményeknek, munkavállalói kötelezettségeknek a betartását ellenőrizze, a fokozatosság elvének betartásával. A munkáltató ellenőrzése során a jogviszony teljesítéséhez használt számítástechnikai eszközön tárolt, a jogviszonnyal összefüggő adatokba tekinthet be. Olyan mélységben tekinthet be, amíg el nem tudja dönteni, hogy az adat magáncélú-e. Amennyiben igen, nem tekinthet be az adatokba.

Adatkezelő vagy harmadik fél jogos érdeke érvényesítéséhez szükséges jogalap szerinti adatkezelések lehetnek pl. a következők: munkahelyi megfigyelő rendszer, munkáltató által biztosított informatikai eszközök, gépjármű adatainak ellenőrzése, munkáltatói e-mail cím/fiók, internet és wifi használatának ellenőrzése, stb. (az aktuális Adatkezelési tájékoztató szerint).

3.2. Ügyfelekkel, szakfeladatokkal kapcsolatos adatkezelések

Az ügyfelekkel és szakfeladatokkal kapcsolatos adatkezelések is akkor jogszerűek, ha 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.

Közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges adatkezelés:

Ha az adatkezelésre közérdekű feladat végrehajtásához, illetve közhatalmi jogosítvány gyakorlásához szükséges, az adatkezelésnek az uniós jogban vagy valamely tagállam jogában foglalt joggal kell rendelkeznie, egyetlen jogszabály szolgálhat jogalapul több adatkezelési művelethez. Az adatkezelés célját uniós vagy tagállami jogban kell meghatározni, melyek pontosíthatják az adatkezelő megjelölésére vonatkozó szabályokat, az adatkezelés tárgyát képező személyes adatok típusát, az érintetteket, azokat a szervezeteket, amelyekkel a személyes adatok közölhetők, az adatkezelés céljára vonatkozó korlátozásokat, az adattárolás időtartamát, valamint egyéb, a jogszerű és tisztességes adatkezelés biztosításához szükséges intézkedéseket is meghatározhatják.

A Szikszó Város Önkormányzata az érintettek tájékoztatóit a GDPR Reg Adatkezelési rendszerben készíti el az előzetesen egyedileg összeállított, folyamatosan aktualizált adatkezelések adataival.

A szerkeszthető adatkezelési tájékoztatók kategóriánként generálhatók, abból a célból, hogy adatkezelő személyre szabott tájékoztatóval tudja tájékoztatni az érintetteket (készülnek munkavállalói, ügyfelekkel kapcsolatos, és szakmai, valamint egyedileg létrehozott kategóriával kapcsolatos adatkezelési tájékoztatók, ha vannak), azok tartalmazzák az érintettek tájékoztatására szolgáló valamennyi rendelkezésre álló információt.

Az Ügyfelekkel kapcsolatos aktuális adatkezelési tájékoztató honlapon kerül publikálásra, ennek megkönnyítésére lehetséges a tájékoztatót tartalmazó weboldal domain nevéhez egyedi ún. API kód generálása. A weboldalt üzemeltető által elvégzett egyszeri kódbeillesztést követően automatikusan megjelenik a weboldalon a Szervezet ügyfelekkel kapcsolatos aktuális adatkezelési tájékoztatója.

3.2.1. Okmánymásolás

Adatkezelésnek minősül a személyes adatokon vagy adatállományokon végzett bármely művelet vagy műveletek összessége, így az adathordozóról készült másolatkészítés vagy a másolatoknak a bekérése is. Az adatkezelések során figyelembe kell venni az adattakarékosság és a célhoz kötött adatkezelés elvét, a személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból, és az adatok kezelése csak e célokkal összeegyeztethető módon történhet, a kezelt adatoknak az adatkezelési cél szempontjából megfelelőnek és relevánsnak kell lenniük, és a kezelt adatok körét a szükségesre kell korlátozni.

Az okmánymásolás csak akkor tekinthető jogszerűnek, ha az általuk gyűjtött adatok kezelésének szükségszerűségét az adatkezelő bizonyítani tudja. A bemutatott érvényes, személyazonosító okmányban szereplő személyazonosító adatokat a dokumentum közhiteles voltára tekintettel másolatkészítés nélkül is el kell fogadni. A személyazonosság igazolására alkalmas hatósági igazolványról készített másolat nem rendelkezik bizonyító erővel arról, hogy hiteles másolata egyérvényes hatósági okmánynak, és nem alkalmas a személyazonosság megállapítására sem. A fényképes igazolvány személyazonosítás céljából való bemutatása felel meg a hatályos jogszabályi rendelkezéseknek, a másolatok kezelése nem felel meg a célhoz kötöttség és az adattakarékosság követelményének. A bemutatott és az adatkezelő ügyintézője, munkatársa által szemrevételezett okmányokból rögzített személyes adatok helyességének utólagos ellenőrizhetősége önmagában nem tekinthető olyan jognak vagy kötelezettségnek, amely az adatkezelés jogszerűségét igazolhatná. A bemutatott érvényes hatósági igazolványokban szereplő adatokat a dokumentumok közhiteles voltára tekintettel másolatkészítés nélkül is el kell fogadni.

4. Technikai és szervezési intézkedések

A Szikszó Város Önkormányzata vezetője felelős azért, hogy figyelembe véve a szervezet méretét, a folyamatok bonyolultságát és kölcsönhatását, a személyzet kompetenciáját, valamint a vonatkozó törvényeket, előírásokat, elvárásokat, meghatározza informatikai- és adatbiztonsági követelményrendszerét és környezetét.

Jelen Adatvédelmi és adatbiztonsági szabályzat jóváhagyásával és hatályba léptetésével biztosítja, hogy az irányítása alatt eljáró, a személyes adatokhoz hozzáféréssel rendelkező természetes személyek kizárólag az utasításának megfelelően kezelhessék az említett adatokat, kivéve, ha az ettől való eltérésre uniós vagy tagállami jog kötelezi őket.

Elkötelezett, hogy a tudomány és technológia állása és a megvalósítás költségei, továbbá 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 hajtson végre annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja.

A Szikszó Város Önkormányzata az egyedi adminisztratív, fizikai és logikai védelmi intézkedéseket az alábbiakban határozza meg, erőforrásainak megfelelően törekszik a betartásukra, betartatásukra:

4.1. Adminisztratív védelmi intézkedések

- A Szervezet feladata a személyes adatokhoz, személyes adatokat tartalmazó dokumentumokhoz, az elektronikus információs rendszerhez hozzáféréssel rendelkező személyek (beleértve a külső személyeket, pl. üzemeltetőket is) folyamatos oktatásának, képzésének elősegítése, az ajánlott elektronikus információbiztonsági eljárások, technikák és technológiák naprakészen tartása. Cél, hogy a felhasználók tudatában legyenek az adatvédelmi és információbiztonsági elvárásoknak és fenyegetettségeknek, illetve felelősségeiknek (pl. jelentési kötelezettségüknek). A biztonság tudatosítása a felhasználók esetében oktató anyagok terjesztésével és képzések útján történik.
- Megismerteti és betartatja munkavállalóival, szerződéses partnereivel, harmadik felekkel - akik hozzáférnek személyes adatokhoz - a személybiztonsági eljárásrendet, szabályzatait, utasításait, az internethasználattal és az elektronikus levelezéssel, az elektronikus információs rendszerhez hozzáférési jogosultságot igénylő személyekkel, felhasználókkal szembeni elvárásokat, szabályokat, felelősségüket, az adott rendszerhez kapcsolódó kötelező, vagy tiltott tevékenységeket.
- Titoktartási nyilatkozat aláírására kötelezi őket, külső fél közötti jogviszony alapjául szolgáló megállapodásban rendelkezik a külső fél titoktartási kötelezettségéről.
- A jogviszony megszűnésekor az alkalmazottnak, bármely jogviszony alapján foglalkoztatottnak, szerződőnek, harmadik félnek az információkhoz és információ-feldolgozó eszközökhöz való hozzáférési jogosultságát megszünteti, visszaveszi az érintett személynek kibocsátott egyéni hitelesítő, hitelesítésre szolgáló eszközöket, felhasználói kártyákat, belépésre jogosító kártyákat (ha vannak), amikor alkalmazásuk megszűnik, szerződésük, illetve megállapodásuk lejár.
- Gondoskodik arról, hogy a tárolt adatokhoz belső rendszeren keresztül vagy közvetlen hozzáférés útján kizárólag az arra feljogosított személyek, kizárólag az adatkezelés céljával összefüggésben férjenek hozzá.
- A felhasználókat tudatosítja, hogy a tőle elvárható gondossággal kell eljárnia az adatkezelés során. Meg kell akadályoznia a kapott hozzáférési jogokkal való visszaélést azáltal, hogy megőrzi a hozzáférési

adatok titkosságát, a felhasználó elszámoltatható minden olyan tevékenységért, amelyet a saját felhasználói azonosítójával végzett, vagy végeztek.

- A szerepkörök és jogosultságok változtatását, változáskezelés keretében hajtja végre, és a szükséges dokumentumokat módosítja (pl. szerződésben meghatározott szerepkör, feladatok, jogok és kötelezettségek, munkaköri leírás).
- Olyan mentési megoldásokat alkalmaz, illetve működtet, amivel biztosítani tudja, hogy az informatikai eszközök sérülése, meghibásodása, adathordozókon tárolt adatok sérülése, használhatatlanná válása esetén, a kiesett informatikai szolgáltatás elfogadható időn belül visszaállítható, illetve az elveszett adatmennyiség mértéke még kezelhető szinten marad. Azon adatok esetében, amelyek hosszú távú megőrzéséért felelős, a mentéseknek alkalmasnak kell lenni az adatok jogszabályban előírt megőrzési idejének végéig történő visszaállítására.
- Alapvető biztonsági szabályokat határoz meg és tart be:
 - o Eltérő megállapodás hiányában tilos a munkavégzéshez biztosított információtechnológiai vagy számítástechnikai eszköz, rendszer, elektronikus levelezési rendszer használata, a tulajdonában lévő internet hálózat feladatellátáson kívüli használata.
 - o A tulajdonát képező levelező rendszer – engedélyezés hiányában – csak szervezeti célokra alkalmazható. Ha a felhasználó a postafiókjára elektronikus levélben vagy annak mellékletében kapott olyan állományt, amely nem munkavégzéshez kapcsolódik, azt haladéktalanul törölnie kell, a tulajdonában lévő adathordozókra tilos a munkavégzéshez nem kapcsolódó, személyes adatot tartalmazó dokumentum (beleértve a fényképeket is) mentése. A felhasználó felel valamennyi, a címéről elküldött levél rendeltetési helyéért és annak tartalmáért.
 - o Javasolt a felhasználóhoz kötött egyéni, teljes névvel ellátott, a szervezet által használt domain nevű egyedi e-mail-címek létrehozása (vezetéknév.keresztnev@domain.hu).
 - o Levelezés a meghatározott, lehetőleg a Szervezet saját tulajdonú domain névhez kapcsolódó tárhelyén történhet, a meghatározott vagy a tárhely szolgáltató által biztosított levelező rendszer használatával, az ingyenes levelezőrendszerek (pl. freemail, gmail, stb.) használatát lehetőleg technikai korlátozásokkal is tiltani kell. Az archív e-mail-ek elérését központi tárhelyen kell biztosítani.
 - o Tilos más postafiókjához felhatalmazás nélkül hozzáférni, más nevében elektronikus üzenetet küldeni, fogadni.
 - o A levelezési fiókhozáférést biztosító jelszót a felhasználónak titkosan kell kezelni, azt mások tudomására hozni még a munkafolyamat felgyorsítása érdekében is tilos. Jelenteni kell a jelszavak nyilvánosságra kerülésére utaló minden gyanút és körülményt.
 - o Ha a felhasználó nem ismeri a külső rendszerből érkező levél feladóját, akkor az üzenet megnyitása előtt igyekezzen azt beazonosítani, gyanús esetben törölje az üzenetet, illetve jelezze ezt felettesének vagy a rendszergazdának. Amennyiben a megnyitás szükséges annak megállapítására, hogy mi az üzenet célja, úgy ezt megfelelő előrelátással (lehetőleg a belső hálózattól elszeparált számítógépen) tegye, és az esetleges csatolt melléklet megnyitását vírus veszély miatt feltétlenül kerülje, további címzettnek nem küldheti tovább.
 - o Tilos a tulajdonában álló informatikai hálózatán, eszközein a nem engedélyezett felhőszolgáltatás, nem szakmai letöltések, tiltott oldalak, nem kívánt levelezőlisták stb. használata, láncclevelek indítása vagy továbbítása, szerzői jogok megsértése (pl. szoftver nem jogszerű terjesztése), egyéni profitszerzést célzó, a szervezettől eltérő üzleti célú tevékenység és reklám, a hálózat, a kapcsolódó hálózatok, illetve ezek erőforrásainak rendeltetésszerű működését és biztonságát megzavaró,

- veszélyeztető tevékenység, ilyen információknak és programoknak a terjesztése, a hálózat erőforrásaihoz, a hálózaton elérhető adatokhoz történő illetéktelen hozzáférés kísérlete, a hozzáférés átruházása más személy részére, a hálózat erőforrásainak, a hálózaton elérhető adatoknak illetéktelen módosítására, megrongálására, megsemmisítésére vagy bármely károkozásra irányuló tevékenység, a Szervezettel kapcsolatos információk nyilvános internetes oldalakon való illegális közzététele.
- Tilos az elektronikus információs rendszerek biztonsági beállításainak megváltoztatása, illetve a vírusellenőrző és Internet böngésző beállítások módosítása.
 - A kijelölt személy rendszeresen ellenőrzi, hogy a felhasználók számára biztosított az Internet elérést lehetővé tevő szoftverek mentesek a komolyabb biztonsági hibáktól.
 - Az elektronikus levelekben, vagy azok mellékleteként a csatolt állományokat az informatikai rendszer automatikusan ellenőrzi, és a biztonságos üzemeltetést veszélyeztető állományok esetében a használatot, illetve a küldés/fogadást megakadályozza. Az állományok küldésére és fogadására vonatkozó korlátozás kiterjed a rendeltetésszerű- és az észszerű használat kereteit meghaladó méretű állományokra is.
- A Szervezet kötelezettsége, hogy munkáltatói rendelkezéseinek, egyéb szabályoknak, pl. az informatikai biztonságra vonatkozó követelményeknek, munkavállalói kötelezettségeknek a betartását ellenőrizze, ennek érdekében a felhasználók által böngészett oldalak listáját naplózhatja, az általa biztosított informatikai eszközöket, adathordozókat, munkáltatói e-mail-címet/fiókot, internet és wifi használatot ellenőrizheti, melynek célja, hogy a felhasználók Internet használata megfeleljen a biztonsági követelményeinek és jogos érdekeinek.
 - A felhasználót tájékoztatja, tudomásul veteti, hogy a Szervezet informatikai hálózatára, eszközeire vonatkozóan ellenőrzési és felelősségre vonási jogosultsága fennáll, a meghatározott viselkedési szabályok megsértése esetén, az adatvédelmi és elektronikus információbiztonsági szabályokat és az ehhez kapcsolódó eljárásrendeket megsértő személyekkel szemben belső eljárási rend szerint fegyelmi eljárást kezdeményez, illetve érvényesíti a vonatkozó szerződésben meghatározott következményeket, megvizsgálja és szükség szerint alkalmazza az egyéb jogi lépéseket.
 - Ha a tevékenység jellege, vagy jogszabályi követelmények megkövetelik, hogy rendelkezzen olyan tervekkel, melyek lehetővé teszik a rendeltetésszerű működéstől eltérő, rendkívüli helyzetek kezelését, akkor Ügymenet folytonossági tervet (BCP) készít, amelynek célja a legfontosabb (kritikus) folyamatok kiesési idejének minimalizálása, az informatikai rendszer normál állapotának lehető legrövidebb időn belül történő visszaállításán túl az, hogy ezt kockázatokkal arányosan lehessen megvalósítani. Ha szükséges, akkor Katasztrófa-elhárítási tervet készít, amely meghatározza a szervezet információs/informatikai rendszereinek teljes működésének (minden funkcionalitásának) a visszaállítását vagy újra felépítését.
 - A bemutatott hatósági okmányokról törvényi kötelezés alapján készít másolatot. A célhoz kötöttség és az adattakarékosság alapelvének érvényesülése érdekében, az okmány bemutatása mellett, az érintett általi nyilatkozat kitöltése vagy arról feljegyzés készítése, illetve a „négy szem elve” (egy másik ügyintéző is megtekinti az érintett által bemutatott okmányt, és ő is megerősíti a személyazonosságot és a rögzített adatok pontosságát) által gyűjti be a szükséges adatokat. A Hatóság szerint kevésbé korlátozza a magánszférát egy feljegyzés készítése vagy egy nyilatkozat kitöltése, mint az okmányok másolása, a másolat készítése nem tekinthető a magánszféra arányos korlátozásának más, hasonlóan hatékony intézkedésekhez képest. Kényelmi szempontok vagy „gyorsabb ügyintézés” nem indokolhatják a másolat készítését.

4.2. Fizikai védelmi intézkedések

- A Szikszó Város Önkormányzata az elektronikus információs rendszereket és az irattároló helyiségeit fizikailag védett, biztonságos helyre telepíti.
- Lehetőség szerint vagyonvédelmi rendszerekkel, távfelügyeleti szolgáltató felügyeleti rendszerére csatlakozó riasztórendszerrel, ha jogos érdekei indokolják, akkor beléptetőrendszerrel, kamerarendszerrel) is védi az adathordozókat tartalmazó helyiségeit, eszközeit a jogosulatlan fizikai hozzáféréstől.
- Felügyelet alatt tartja az adathordozókat tartalmazó helyiségeket, ügyfelek, látogatók nem tartózkodhatnak kíséret nélkül.
- Alkalmazza az „Üres íróasztal - tiszta képernyő” szabályt:
 - o a monitorok elhelyezésekor törekszik az azokra való minél kisebb rálátás biztosítására, hogy a képernyők tartalma ne legyen olvasható az alkalmilag arra haladó személyek számára, és ne legyen látható az épületen kívülről (ha monitor elhelyezéssel nem biztosítható, akkor sötétítő függöny használatával);
 - o a felhasználó a számítógépét zárolja, ha azt rövidebb időre őrizetlenül hagyja;
 - o a munkafázis végeztével vagy hosszabb idejű távollét esetén a számítógépből kijelentkezik, illetve kikapcsolja;
 - o törekszik arra, hogy munkavégzés után minden érzékeny információt tartalmazó anyagot (papír alapú anyagokat, valamint elektronikus adathordozókat) eltávolít az asztalokról és zárható irodabútorban tárol;
 - o gondoskodik arról, hogy a nyomtatókból, faxokból, fénymásolókból kijövő dokumentumokhoz illetéktelenek ne férjenek hozzá;
 - o ügyel arra, hogy érzékeny információt tartalmazó dokumentumok ne maradjanak a fénymásolóban, a kinyomtatott, faxolt vagy másolt dokumentumokat nem hagy őrizetlenül az eszközökben;
 - o a hibásan nyomtatott, nem használt dokumentumokat megsemmisít (pl. iratmegsemmisítővel).
- A fénymásoló és nyomtató berendezéseket/multifunkcionális nyomatkészítőket, a fax készülékeket és minden egyéb kimentési eszközt védett területen belül helyezi el, ahol a felügyeletük biztosítható, az illetéktelen hozzáférés megakadályozható (harmadik fél, ügyfél és látogatók részére nem hozzáférhetőek), vagy nyilvános zónában PIN kóddal védett nyomtatás kerül beállításra.
- Védi a helyiségeit az adathordozókat károsító behatásoktól (extrém hőmérséklet és páratartalom), az informatikai erőforrásokat koncentráltan tartalmazó helyiségekben (pl. szerverhelyiség) szükség esetén biztosítja a megfelelő környezeti feltételeket.
- Az elsődleges áramforrás kiesése esetére azokhoz a rendszerekhez, ahol az indokolt vagy elvárt (pl. szerverfunkciójú számítógépek, adatmentő szerverek, hálózati eszközök), az eszközök szabályos leállításához a tevékenységhez méretezett, rövid ideig működőképes szünetmentes áramellátást biztosít.
- Azokban a helyiségekben, ahol az indokolt (pl. szerverszobában) független áramellátással támogatott érzékelő berendezést (füstérzékelőt) alkalmaz, azok jelzéseit a vagyonvédelmi rendszer részeként hatósági engedéllyel rendelkező távfelügyeleti szolgáltató felügyeleti rendszerére csatlakoztat.
- Az adatvesztés megelőzése érdekében betartja a tűzvédelmi előírásokat, az informatikai eszközök központi helyiségeibe (elosztó-, szerverhelyiségekbe) és ahol a tűzvédelmi szempontból indokolt, minimális elvárásként tanúsított gázzal oltó (CO₂) hordozható, kézi tűzoltó készülékeket biztosít.

4.3. Logikai védelmi intézkedések

- A Sziksó Város Önkormányzata kizárólag olyan szoftvereket és kapcsolódó dokumentációt használ, amelyek megfelelnek a rájuk vonatkozó szerződésbeli elvárásoknak és a szerzői jogi, vagy más jogszabályoknak.
- Szabályokhoz köti a szoftverek, alkalmazások telepítését, másolását, eltávolítását, a megfelelő biztonsági beállításokat.
- Betartja a hozzáférés ellenőrzési eljárásrendet, az elektronikus információs rendszer, rendszerelem használója kizárólag személy vagy szerződéses jogviszonyban álló szerződött partner, harmadik személy, aki a munkavégzéshez szükséges feltételekkel, megismerte a vonatkozó szabályokat, vonatkozó rendelkezéseket, és ennek megfelelően hozzáférési jogosultságot kapott az elektronikus információs rendszerek használatához.
- A hozzáférési jogosultságok megszüntetéséről szükség esetén intézkedik: kilépés, jogviszony megszűnése, szerződés lejáratát vagy megszűnése, kinevezés visszavonás, szervezeten belüli áthelyezés, munkakör jelentős megváltozása, tartós betegség, távollét, illetve helyettesítés esetén, valamint visszaélés gyanúja vagy hasonló súlyos biztonsági esemény felmerülése esetén.
- Biztosítja, hogy megfelelő jogosultság nélkül senki sem férhet hozzá a Szervezet rendszereihez, illetve olyan számítógépekhez, melyek ügyfél adatokat vagy bizalmas információt, védendő személyes adatokat tartalmaznak. Senki sem végezhet jogosulatlanul bármiféle változtatást az informatikai rendszerekben, beleértve az adatok törlését vagy megváltoztatását is.
- Az illetéktelen használat megakadályozására a munkaállomásokon automatikus képernyővédelmet állít be úgy, hogy felhasználói inaktivitást követően meghatározott időtartalom után automatikusan zárolja a munkaállomást. Az ismételt bejelentkezés kizárólag a felhasználó azonosításával és hitelesítésével történhet (felhasználónév és jelszó megadása).
- Kizárólag indokolt esetben engedélyezi a vezeték nélküli kapcsolaton keresztüli csatlakozást az elektronikus információs rendszeréhez, felhasználói korlátozásokat vezet be.
- Gondoskodik a felhasznált eszközök szükséges, rendszeres karbantartásáról, fejlesztéséről. A karbantartásokat és javításokat ütemezetten, dokumentáltan hajtja vagy hajtattja végre.
- A karbantartásokat, javításokat csak az arra jogosult személyek végzik. Karbantartás céljából az adathordozók, információs rendszer vagy rendszerelem szállítását a rendszergazda, külső személy/szolgáltató esetében a megbízott személy/szolgáltató végzi.
- Gondoskodik arról, hogy a felhasználók, a felhasználók által végzett tevékenységek – az engedélyezett jogosultságoknak megfelelően – egyedileg legyenek azonosítva és hitelesítve, abból a célból, hogy elkerülhetővé váljanak a jogosulatlan hozzáférések, csökkenve a jogosulatlan hozzáférésekből származó információbiztonsági incidenseket.
- Kizárólag a tulajdonában lévő, nyilvántartott adathordozó, illetve behozott adathordozó esetében ellenőrzött és engedélyezett eszköz használatát engedélyezi.
- Az adathordozók használatát egyes informatikai eszközökön információbiztonsági megfontolásból utasítással, hardver, illetve szoftver úton korlátozhatja, figyelheti, monitorozhatja. Engedélyezheti, korlátozhatja vagy tilthatja bizonyos, vagy bármely adathordozó típusok használatát a kijelölt elektronikus információs rendszereken vagy rendszerelemeken működő biztonsági intézkedések használatával.

- Írásos engedélyhez köti az adathordozók, mobil eszközök (laptop, pendrive, floppyn, CD stb.) - otthoni vagy külső helyszínen történő munkavégzés, vagy bármilyen más célból történő - kiszállítását.
- Lehetőség szerint a mobil/szervezeten kívül kiszállításra engedélyezett hordozható eszközöket kriptográfiai (hardver vagy szoftver titkosítási) mechanizmusokkal is védi a digitális adathordozókon tárolt információk bizalmosságának és sértetlenségének védelme érdekében (hordozható adattároló, pl. okostelefon, laptop, pendrive stb.). A kiszállított mobil eszközök esetén eszköztitkosítást, tároló alapú titkosítást, vagy más technológiai eljárást alkalmaz (pl. BIOS jelszó, Win10 Pro esetén BitLocker, ESET Endpoint Encryption). Kizárólag nyilvántartott, hardveres titkosítású pendrive használat engedélyezett.
- Betartatja az adattartalommal bíró adathordozók, információs rendszer vagy rendszerelem szállítása esetén a megfelelő információbiztonsági intézkedéseket. Karbantartás céljából az adathordozók, információs rendszer vagy rendszerelem szállítását a rendszergazda, külső személy/szolgáltató esetében a megbízott személy/szolgáltató végzi.
- Biztosítja, hogy az operációs rendszerek vagy üzletileg kritikus alkalmazások verziófrissítése megtervezett módon történjen meg, a biztonságkritikus szoftverek a frissítésük kiadását követő meghatározott időtartamon belül telepítésre kerüljenek (a frissítések történhetnek automatikusan is az adott operációs rendszer frissítési beállításainak megfelelően). Egyéb biztonsági kockázatot nem jelentő frissítéseket csak abban esetben telepíti, ha azok üzleti szempontból lényeges hibák, sérülékenységek kijavítását, funkcióbővítést eredményeznek.
- Meghatározta és betartatja az adathordozók kezelésének általános irányelveit:
 - o informatikai eszközöket, adathordozókat tilos nyilvános helyen vagy harmadik félnél történő munkavégzés során őrizetlenül hagyni;
 - o munkavégzés közben nem lehet a használatban lévő mobil eszközöket felügyelet nélkül hagyni, a használaton kívüli eszközöket védett helyen kell tárolni („tiszta asztal” szabálya);
 - o az informatikai infrastruktúra elemeit engedély nélkül, nem a munkaköri feladatba tartozó módon megváltoztatni, vagy eltávolítani nem lehet;
 - o tilos az olyan hordozható adathordozó használata az elektronikus információs rendszerben, melynek tulajdonosa nem azonosítható. Az adathordozókat sorszámmal és/vagy a felügyeletéért felelős nevével azonosítani kell, azokat a felhasználóhoz kell rendelni;
 - o az adathordozókat a felhasználók nem csatlakoztathatják egymás eszközeihez úgy, hogy az eszköz tulajdonosa nem tud róla;
 - o amennyiben kívülről érkezik adat valamilyen adathordozón, annak a megtekintése csak előzetes ellenőrzés és a vírus mentesség megállapítása után használható;
 - o bármely adathordozó eltűnését azonnal jelenteni kell a Szervezet vagy szervezeti egység vezetőjének, a továbbiakban az adatvédelmi incidensként kell kezelni a 2.6. fejezet szerint.
- Betartja az adathordozók törlésére vonatkozó biztonsági irányelveket:
 - o az adathordozókat elhasználódásuk esetén cserélni és selejtezni kell az adatvesztés elkerülése érdekében,
 - o az adathordozókat selejtezés, a szervezeti ellenőrzés megszűnte, vagy újrafelhasználásra való kibocsátás előtt dokumentáltan adatmentesíteni kell ilyen célú megfelelő alkalmazással,
 - o a nem törölhető adathordozókat meg kell semmisíteni iratmegsemmisítőben vagy más módon össze kell törni,

- a törlési mechanizmusokat az információ minősítési kategóriájával arányos erősségnek és sértetlenségnek megfelelően kell alkalmazni, biztosítva, hogy a megsemmisítési eljárások során az kimeneti információk tartalma helyreállíthatatlanul megsemmisüljön.
- Meghatározta és érvényesíti a felhasználó számítógépes szolgáltatásokhoz való hozzáférési jogosultságának hitelesítésére szolgáló jelszavak kezelésével kapcsolatos elvárásait:
 - a munkaállomások, rendszerelemek, rendszerek hozzáféréséhez szükséges jelszavakat a jelszavak erősségének irányelve alapján kell megadni (figyelembe véve a jelszavak kompromittálásából adódó kockázatokat);
 - a jelszavak erősségének irányelve: a jelszavak minimális hossza 6 karakter, tartalmazniuk kell kis- és nagybetűket, speciális és numerikus karaktereket egyaránt. Tilos olyan jelszavakat alkalmazni, melyek könnyen kitalálhatóak, mint például a személyes adatok, egyértelmű dátumok, gépnévre vagy a felhasználói névre utalóak vagy általános, szótári szavak (pl. „admin”, „password”), illetve amelyek gyári beállítású, alapértelmezett jelszavak;
 - a munkaállomásokhoz, rendszerelemekhez, információs rendszerekhez kiadott kezdő jelszavakat kötelező az első bejelentkezés alkalmával megváltoztatni;
 - a felhasználók és megbízott harmadik felek felelősek a személyes jelszavaik megfelelő védelméért és annak következményeiért, ha a jelszavaik mások által ismertté válnak;
 - a jelszavakat azonnal meg kell változtatni, ha a felhasználó úgy gondolja, hogy azok más tudomására jutottak, vagy valami szokatlan tapasztaltak a számítógépes rendszerükben (ezt követően értesíteni kell a rendszergazdát és az elektronikus információs rendszer biztonságáért felelős személyt);
 - a jelszavakat rendszeres időközönként cserélni kell (lehetőség szerint automatikusan kikényszerítve), illetve az elektronikus információs rendszer által kikényszerített, vagy az üzemeltetők által meghatározott időközönként;
 - új jelszónak nem szabad az utolsó 5 régebbi közül egyiket sem megadni;
 - a jelszavakat alapvetően tilos leírni;
 - nem tehető a jelszó egy automatikus bejelentkezési folyamat részévé;
 - tilos a felhasználóknak bejelentkezni olyan felhasználónévvel, melyet eredetileg nem nekik bocsátottak ki, és amelyek használatára nem jogosultak;
 - amennyiben a felhasználók által használt rendszerek valamelyike a fentieknél alacsonyabb biztonsági szintet követelne meg, a felhasználóknak minden esetben az itt szereplő szabályok szerint kell eljárni;
 - ez a jelszó politika érvényes azokra a külső rendszerekre is, amelyeket a felhasználók a munkájukkal kapcsolatosan elérnek.
- Amennyiben erre lehetőség van, a folyamatos ügymenet biztosítása érdekében beállítja az egyes informatikai rendszerekben a helyettesítéseket, vagy biztosítja, hogy az egyes rendszerekhez több felhasználónak legyen kiosztva jogosultsága.
- Törekszik a legkisebb jogosultság kiosztásához. Valamennyi felhasználó munkavégzése során a szükséges és elégséges hozzáférés elve alapján kizárólag a feladat ellátásához szükséges adat, információ megismerésére, továbbá az adat- és rendszerhozzáférésre a munkavégzéséhez szükséges lehető legrövidebb ideig és szükséges legkisebb jogosultsági szint alkalmazásával jogosult. A szükséges mértékre és időtartamra történő korlátozás nemcsak a hozzáférés kockázatát minimalizálja, hanem a hozzáférő személy által viselt felelősséget is.
- A hitelesítésre vonatkozó követelményeket valamennyi rendszerelemre vonatkozóan érvényesíti.

- A menedzselhető hálózati aktív eszköz tekintetében az eszköz gyári, alapértelmezett bejelentkezési azonosítóit (név, password) megváltoztatja. Csak előre kijelölt, privilegizált felhasználóknak van lehetősége bejelentkezni az eszközökbe.
- Megfelelő védelmi szoftverek és eszközök (tűzfal, vírusirtó) alkalmazásával és az alkalmazások biztonsági beállításával mindent megtesz a rosszindulatú programok károkozásával szemben.
- A munkaállomásokon lévő víruskeresőt úgy állítja be, úgy üzemelteti, hogy az automatikusan ellenőrizze a munkaállomásra csatlakoztatott adathordozókat, akadályozza meg a vírusok adathordozón, vezetékes vagy vezeték nélküli hálózaton, elektronikus levelezésben, vagy internet használat során történő bejutását a rendszerekbe, rendszeres ellenőrzéseket hajtson végre a belépési/kilépési pontokon, szükség esetén automatikusan riassza a rendszergazdát vagy a meghatározott további személyeket. Az esetlegesen mégis bejutott vírusok kártételének meggátlása céljából a rendszereket lehetőleg automatikusan, a felhasználó beavatkozását nem igénylő módon, rendszeresen át kell vizsgálni, és a bejutott kártékony kódokat meg kell semmisíteni.
- Megtiltja, hogy az elektronikus postafiókba érkező, ismeretlen feladótól származó, nem szokványos formátumú, gyanús csatolmányt tartalmazó, illetve idegen nyelvű küldemények, vagy a vírusvédelmi rendszer riasztása esetén bármely állomány, weboldal megnyitásra kerüljön.
- A szükséges mértékben naplózza a személyes adatok hozzáféréseit, valamint a biztonsági eseményeket.
- Szükség esetén belső engedélyhez köti az elektronikus információs rendszerek kapcsolódását más elektronikus információs rendszerekhez, dokumentálja az egyes kapcsolatokat, az interfészek paramétereit, a biztonsági követelményeket és a kapcsolaton keresztül átvitt elektronikus információk típusát.
- A saját hatókörben beszerzett rendszerekre, rendszerelemekre vonatkozóan az elektronikus információs rendszereinek teljes életútján, azok minden életciklusában figyelemmel kíséri informatikai biztonsági helyzetüket. Folyamatosan fel kell térképezni az összes üzemelő, használatban lévő vagy a jövőben bevezetésre tervezett informatikai eszközt, rendszert, a kezelt adatokat, a kezelt személyes adatokat és mindezek környezetét alkotó összes rendszerelemet (azok teljes életciklusában a tervezéstől, elkészítéstől, a rendszerből történő teljes kivonásáig, vagy megsemmisítésig).
- A legszűkebb funkcionalitás érdekében az elektronikus információs rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztője, illetve üzemeltetője az elektronikus információs rendszert úgy konfigurálja, hogy az csak a szükséges szolgáltatásokat nyújtsa.
- Saját hatókörén belül meghatározza és biztosítja azokat a minimum konfigurációs beállításokat, amelyek a munkavégzéshez szükségesek. Ennek köszönhetően, semmilyen felesleges beállítás, plusz szolgáltatás/funkció nem kerül konfigurálásra.
- Korlátozza egyes szoftverek és szolgáltatások hozzáférését. Tiltja egyes portok, protokollok elérhetőségét elkerülve ezzel a külső támadásokat. Szükséges mértékben korlátozza a külső portok (pl. usb) használatát.

4.4. Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény hatálya alá tartozó szervek további követelményei

Az lbtv. hatálya alá tartozó állami és önkormányzati szervezeteknek teljesíteni kell a 2013. évi L. törvény, valamint a törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet Védelmi intézkedések fejezetben felsorolt, az informatikai rendszerek biztonsági osztályához tartozó adminisztratív, fizikai és logikai védelmi intézkedéseket, illetve a központi szolgáltató (a jogszabály által kijelölt központosított informatikai és elektronikus hírközlési szolgáltató) előírásait. A betartandó követelményeket az *Informatikai biztonsági szabályzat* tartalmazza részletesen.

Az elektronikus információs rendszer biztonságáért felelős személy felel a Szervezetnél előforduló valamennyi, az elektronikus információs rendszerek védelméhez kapcsolódó feladat ellátásáért.

Az lbtv. 3. § (2) -(3) bekezdése alapján a külföldi adatkezelést, az egyes elektronikus információs rendszerek Magyarország területén kívül üzemeltetését előzetesen engedélyeztetni kell (pl. honlap üzemeltetés, email szerver).Lásd 2.8.1. *Adattovábbítás harmadik országokba* fejezetet.

Fogalomtár

A meghatározások megfelelnek az Európai Parlament és a Tanács (EU) 2016/679 rendeletében és az információs önrendelkezési jogról és információszabadságról szóló 2011. évi CXII. törvényben használt kifejezéseknek:

- adatállomány:** az egy nyilvántartásban kezelt adatok összessége;
- adatifeldolgozás:** az adatkezelő megbízásából vagy rendelkezése alapján eljáró adatifeldolgozó által végzett adatkezelési műveletek összessége;
- adatifeldolgozó:** az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel;
- adatfelelős:** az a közfeladatot ellátó szerv, amely az elektronikus úton kötelezően közzeendő közérdekű adatot előállította, illetve amelynek a működése során ez az adat keletkezett;
- adatkezelés korlátozása:** a tárolt személyes adatok megjelölése jövőbeli kezelésük korlátozása céljából;
- adatkezelés:** a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés;
- adatkezelő:** az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza (15725723); ha az adatkezelés céljait és eszközeit az uniós vagy a tagállami jog határozza meg, az adatkezelőt vagy az adatkezelő kijelölésére vonatkozó különös szempontokat az uniós vagy a tagállami jog is meghatározhatja;
- adatközlő:** az a közfeladatot ellátó szerv, amely – ha az adatfelelős nem maga teszi közzé az adatot – az adatfelelős által hozzá eljuttatott adatot honlapon közzéteszi;
- adatmegsemmisítés:** az adatot tartalmazó adathordozó teljes fizikai megsemmisítése;
- adattovábbítás:** az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele;
- adattörlés:** az adat felismerhetetlenné tétele oly módon, hogy a helyreállítása többé nem lehetséges;
- 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;
- 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;
- azonosítható természetes személy:** az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, azonosító szám, helymeghatározó adat, online azonosító vagy a természetes személy fizikai, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható;

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 2016.5.4. L 119/33 Az Európai Unió Hivatalos Lapja HU 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;

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;

érintett hozzájárulása: az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez;

érintett: bármely információ alapján azonosított vagy azonosítható természetes személy;

felügyeleti hatóság: egy tagállam által az 51. cikknek megfelelően létrehozott független közhatalmi szerv. Magyarországon a NAIH (Nemzeti Adatvédelmi és Információszabadság Hatóság), mint az Infotv. által 2012. január 1-vel létrehozott, az adatvédelmi biztos intézményét felváltó nemzeti adatvédelmi hatóság. Feladata a két információs jog védelme és a magyarországi adatkezelések törvényességének felügyelete;

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;

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;

harmadik ország: minden olyan állam, amely nem EGT-állam;

hozzájárulás: az érintett akaratának önkéntes, határozott és megfelelő tájékoztatáson alapuló egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy az akaratát félreérthetetlenül kifejező más magatartás útján jelzi, hogy beleegyezését adja a rá vonatkozó személyes adatok kezeléséhez;

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

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;

közérdekből nyilvános adat: a közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli;

közérdekű adat: az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő és tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől, így különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre, annak eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat;

közös adatkezelő: az az adatkezelő, aki vagy amely – törvényben vagy az Európai Unió kötelező jogi aktusában meghatározott keretek között – az adatkezelés céljait és eszközeit egy vagy több másik adatkezelővel közösen határozza meg, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket egy vagy több másik adatkezelővel közösen hozza meg és hajtja végre vagy hajtatja végre az adatfeldolgozóval;

közvetett adattovábbítás: személyes adatnak valamely harmadik országban vagy nemzetközi szervezet keretében adatkezelést folytató adatkezelő vagy adatfeldolgozó részére továbbítása útján valamely más harmadik országban vagy nemzetközi szervezet keretében adatkezelést folytató adatkezelő vagy adatfeldolgozó részére történő továbbítása;

különleges adat: a személyes adatok különleges kategóriába tartozó minden adat, azaz a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a genetikai adatok, a természetes személyek egyedi azonosítását célzó biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok;

nemzetközi szervezet: a nemzetközi közjog hatálya alá tartozó szervezet vagy annak alárendelt szervei, vagy olyan egyéb szerv, amelyet két vagy több ország közötti megállapodás hozott létre vagy amely ilyen megállapodás alapján jött létre;

nyilvánosságra hozatal: az adat bárki számára történő hozzáférhetővé tétele;

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 helyzetéhez, egészségi állapothoz, személyes preferenciákhoz, érdeklődéshez, megbízhatóságához, viselkedéshez, tartózkodási helyhez vagy mozgáshoz kapcsolódó jellemzők elemzésére vagy előrejelzésére használják;

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

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.



Szikszó Város Önkormányzata
3800 Szikszó, Kálvin tér 1.
Tel:(46) 596-450; Fax:(46) 596-211
info@szikso.hu

HATÁROZAT

17/2020.(V.29.) Szikszó Város Önkormányzat Polgármesteri Határozata

Szikszó Város Önkormányzat Polgármestere a veszélyhelyzet kihirdetéséről szóló 40/2020. (III.11.) számú kormányrendelet, valamint a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény 46.§ (4) bekezdésében foglalt jogköre alapján a Képviselő-testület feladat- és hatáskörében eljárva az alábbiak szerint határoz:

Döntés Szikszó Város Önkormányzatának Közterületi térfigyelő kamerarendszer adatvédelmi szabályzatának elfogadásáról

Szikszó Város Önkormányzat Polgármestere úgy határoz, hogy elfogadja 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 (EU) 2016/679 rendelet (Általános adatvédelmi rendelet vagy GDPR) és az Információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény alapján a határozat mellékletét képező Közterületi térfigyelő kamerarendszer adatvédelmi szabályzatot Szikszó Város Önkormányzatára vonatkozóan.
(Írásos anyag csatolva: 4. sz. melléklet)

Felelős: polgármester
Határidő: azonnal

Kelt: Szikszó, 2020.05.29.





Szikszó Város Önkormányzata

Közterületi térfigyelő kamerarendszer adatvédelmi szabályzat, tájékoztató

Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.)
a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről
és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül
helyezéséről (általános adatvédelmi rendelet) szerint

érvényes:

2020.05.29

jóváhagyta:



Sváb Antal Béla

1. Adatkezelő, adatfeldolgozó

Térfigyelő kamerarendszer tulajdonosa, a térfigyelő kamerarendszer üzemeltetője:

Név: Szikszó Város Önkormányzata
Székhely: 3800 Szikszó, Kálvin tér 1.
Polgármester: Sváb Antal Béla
Adatvédelmi tisztviselő neve: Juhász Gergely
Telefon: +36 46 596444
E-mail: adatvedelem@szikso.hu

Szikszó Város Önkormányzata a közterület-felügyelet (a továbbiakban: felügyelet) feladatait a polgármesteri hivatalban alkalmazott egy vagy több közterület-felügyelő látja el.

Név: Szikszó Város Önkormányzata
Székhely: 3800 Szikszó, Kálvin tér 1.

2. Adatkezelésre vonatkozó jogforrások, egyéb szabályzatok

- Magyarország Alaptörvénye
- Közterület-felügyeletről szóló 1999. évi LXIII. törvény (továbbiakban: Kftfv.)
- A polgárőrségről és a polgárőri tevékenység szabályairól szóló 2011. évi CLXV. törvény (továbbiakban Pötv.)
- A Rendőrségről szóló 1994. évi XXXIV. törvény (továbbiakban Rtv.)
- Magyarország helyi önkormányzatairól szóló 2011. évi CLXXXIX. törvény (továbbiakban Möt.)
- Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben (a továbbiakban Ibtv.)
- Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (a továbbiakban: általános adatvédelmi rendelet)
- Az információs önrendelkezési jogról és információszabadságról szóló 2011. évi CXII. törvény (továbbiakban Infotv.)
- Kapcsolódó főbb belső szabályzatok:
 - Adatvédelmi és adatbiztonsági szabályzat
 - Üzemeltetési szabályzat, utasítás

3. A szabályzat, tájékoztató célja, hatálya

Jelen szabályzat, tájékoztató fő célja, hogy Adatkezelő a létesített térfigyelő kamerarendszer adatkezeléssel kapcsolatos tevékenységéről tájékoztassa az érintetteket - a képrögzítő eszközön a megfigyelt területre belépőket, vagy akinek jogát vagy jogos érdekét a felvétellel rögzített esemény, cselekmény vagy intézkedés érinti -, elősegítve az általános adatvédelmi rendeletnek és az információs önrendelkezési jognak az érvényesülését, és az érintetti jogok gyakorlását.

A szabályzat, tájékoztató kiegészíti az Adatvédelmi és adatbiztonsági szabályzatot, adatkezelési tájékoztatókat, azokkal összhangban készül, Adatkezelő gondoskodik azok folyamatos összhangjáról.

Az adatrögzítésre, a rögzített adatok felhasználására, az adattovábbításra, betekintésre, adattörlésre, a nyilvántartások vezetésére, a személyes adatok védelmére vonatkozó részletes szabályokat, további szervezési, technikai és egyéb intézkedéseket külön szabályzat, utasítás tartalmazza.

Adatkezelő vezetőjének felelőssége, hogy az adatkezelésben érintett munkatársak, közreműködők, akik az adatkezeléssel kapcsolatos folyamatokban, tevékenységekben bármi módon részt vesznek, ismerjék és betartsák a rájuk vonatkozó elvárásokat, kötelezettségeket.

A szabályzat, tájékoztató hatálya a közterületen vagy az önkormányzat illetékességi területén elhelyezett és Adatkezelő által kezelt és üzemeltett térfigyelő kamerarendszerre terjed ki.

Jelen szabályzat, tájékoztató a kiadás napján lép hatályba, mellyel valamennyi korábbi e tárgyú szabályzat, tájékoztató hatályát veszti.

4 Térfigyelő kamerarendszer létesítése

Helyi önkormányzati feladat a helyi közügyek, valamint a helyben biztosítható közfeladatok körében a település közbiztonságának biztosításában való közreműködés (Mötv. 13. § (1) 17. pontja).

A települési önkormányzat a közterületi rend és tisztaság, az önkormányzati vagyon védelméről a Kfttv. 1. § (1) bekezdése alapján közterület-felügyelet vagy közterület-felügyelő útján is gondoskodhat.

A Kfttv. 7. § (3) bekezdése alapján közterületen, közbiztonsági, illetve bűnmegelőzési célból, bárki számára nyilvánvalóan észlelhető módon képfellevőt helyezhető el és felvétel készíthető.

Szikszó Város Önkormányzata Képviselő-testülete az Alaptörvény 32. cikk (2) bekezdésében meghatározott eredeti jogalkotói hatáskörben a közterület-felügyeletről szóló 1999. évi LXIII. törvény 7. § (3) bekezdésében, valamint a Magyarország helyi önkormányzatairól szóló 2011. évi CLXXXIX törvény 13. § (1) bekezdés 17. pontjában meghatározott feladatkörében eljárva döntött a képfellevő elhelyezéséről, valamint a képfellevővel megfigyelt közterület kijelöléséről.

Ez alapján Szikszó Város közigazgatási területén, közterületen - ahol az közbiztonsági, bűnmegelőzési, illetve bűnüldözési célból igazolhatóan szükséges - bárki számára nyilvánvalóan észlelhető módon közterületi térfigyelő rendszert működtet, képfellevőt helyez el és felvételt készít, tárol, kezel.

A képfellevő által megfigyelt területre belépő személyek tájékoztatását elősegítő módon figyelemfelhívó jelzést, ismertetést helyez el a képfellevők elhelyezéséről, az adatkezelés tényéről.

A képfellevők elhelyezésére, a megfigyelt területre vonatkozó adatokat (a kamerák pontos helyszínét, elhelyezését, megfigyelés módját) a település honlapján a Közterület-felügyeletről szóló 1999. évi LXIII. törvény 7. § (4) bekezdése alapján közzéteszi (1. melléklet), valamint arról tájékoztatja a rendőrséget.

Adatkezelő a jogszabályban meghatározottak szerint együttműködik a Kormány által kijelölt központi tárhelyszolgáltatóval. A felvételeket – amennyiben annak műszaki és technikai feltételei adottak – a Kormány által kijelölt központi tárhelyszolgáltató által biztosított tárhelyen rögzíti.

5. Értelmező rendelkezések

A szabályzat, tájékoztató alkalmazása során az egyes fogalmakon a következőket kell érteni, különösen a GDPR 4. cikk értelmében használt adatvédelmi kifejezéseket:

Közterületi térfigyelő kamerarendszer: Azok az eszközök és megoldások, melyek kamerák kihelyezésével és üzemeltetésével lehetővé teszik a közterület távolból történő megfigyelését, a kamerákkal képfelvételek készítését, a felvételek tárolását, kezelését, az adatok továbbítását.

Kamerarendszer részei:

- közterületre kihelyezett kamerák,
- központi megfigyelő, illetve rögzítő helyiség a szükséges eszközökkel és műszaki megoldásokkal

Közterület: A közhasználatra szolgáló minden olyan állami vagy önkormányzati tulajdonban álló terület, amelyet rendeltetésének megfelelően bárki használhat, ideértve a közterületnek közútként szolgáló és a magánterületnek a közforgalom számára a tulajdonos (használó) által megnyitott és kijelölt részét, továbbá az a magánterület, amelyet azonos feltételekkel bárki használhat.

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

Érintett: Bármely információ alapján azonosított vagy azonosítható természetes személy.

Adatkezelő: Az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza (15725723). Ha az adatkezelés céljait és eszközeit az uniós vagy a tagállami jog határozza meg, az adatkezelőt vagy az adatkezelő kijelölésére vonatkozó különös szempontokat az uniós vagy a tagállami jog is meghatározhatja.

Adatkezelés: A személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés, továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés.

Adattovábbítás: Az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele.

Adatfeldolgozó: Az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel.

Nyilvánosságra hozatal: Az adat bárki számára hozzáférhetővé tétele.

Adattörlés: Az adat felismerhetetlenné tétele oly módon, hogy a helyreállítása többé nem lehetséges.

Adatmegsemmisítés: Az adatot tartalmazó adathordozó teljes fizikai megsemmisítése.

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.

6. A személyes adatok kezelésére vonatkozó elvek

Jogszerűség, tisztességes eljárás és átláthatóság: A személyes adatok kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni.

Célhoz kötöttség: A személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történjen, és azokat ne kezeljék ezekkel a célokkal össze nem egyeztethető módon. Nem minősül az eredeti céllal össze nem egyeztethetőnek a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból történő további adatkezelés.

Adattakarékosság: A személyes adatok az adatkezelés céljai szempontjából megfelelőek és relevánsak kell, hogy legyenek, és a szükségesre kell korlátozódniuk.

Pontosság: A személyes adatoknak pontosnak és szükség esetén naprakésznek kell lenniük. Minden ésszerű intézkedést meg kell tenni annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul töröljék, vagy helyesbítsék.

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 kezelésére közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból kerül majd sor, az érintettek jogainak és szabadságainak védelme érdekében előírt megfelelő technikai és szervezési intézkedések végrehajtására is figyelemmel.

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.

Elszámoltathatóság: Az adatkezelő felelős a fenti alapelveknek való megfelelésért, továbbá képesnek kell lennie e megfelelés igazolására.

7. Adatkezelés célja

A térfigyelő rendszer üzemeltetés célja a Közterület-felügyeletről szóló 1999. évi LXIII. törvényben meghatározott célok közül különösen a település közbiztonságának növelése, a jogellenes köztéri magatartások megelőzése, felderítésük elősegítése, visszaszorítása, a közterületi rendre vonatkozó előírások betartásának ellenőrzése, az önkormányzati vagyon védelme, mindezek által a lakosság biztonságérzetének erősítése.

A megfigyelt területre belépő és ott tartózkodó személyekről készülő képfelvételek rögzítésének és felhasználásának további célja lehet a bűnüldöző tevékenység segítése, a bűnüldözésben, bűnmegelőzésben az állampolgárok személyi és vagyonbiztonságának növelésében tevékenykedő szervezetek közötti együttműködés elősegítése, a rögzítés helyszínén a felvételen szereplő személy által, jogainak gyakorlása érdekében indított eljárásban történő felhasználása céljából, illetve körözött személy vagy tárgy azonosítása érdekében.

A képfelvételeket a települési önkormányzat vagy rendőrség szükség esetén felhasználhatja a törvényben meghatározott feladatainak ellátásához.

8. A kezelt adatok köre, forrása

A képrögzítő eszközön a megfigyelt területre belépők képmása, tevékenysége, mint személyes adatnak is minősülő felvételek kerülnek rögzítésre, tárolásra. A felvételen beazonosítható természetes személyek jelenhetnek meg, különböző mozgást, magatartást megvalósítva, amelyből közvetett vagy közvetlen következtetések is levonhatóak. Amennyiben a kamerarendszer által rögzített adatok felhasználásra kerülnek, akkor személyes adatnak tekinthető az érintett magatartása is, mint az érintettre vonatkozó következtetés.

Az adatok az érintettől, a képfelvevő eszközzel megfigyelt területen tartózkodó természetes személyektől származnak, a képfelvevő eszközök látómezeje szerint, lásd 1. sz. melléklet.

A térfelügyelő kamerák, képfelvevők kizárólag közterületen - ahol az közbiztonsági, bűnmegelőzési, illetve bűnüldözési célból igazolhatóan szükséges, bárki számára nyilvánvalóan észlelhető módon - kerültek elhelyezésre, a kamerával nem kerül sor magánterület megfigyelésére. Ha ezt a feltételt a kamera beállításával nem lehet teljesíteni, akkor maszkolással kell leszűkíteni a kamerák látómezejét, ki kell takarni az inkriminált területeket.

9. Adatkezelés jogalapja

A térfelügyelő rendszerrel kapcsolatos adatkezelés jogalapja az Európai Parlament és a Tanács (EU) 2016/679 rendelete (általános adatvédelmi rendelet) 6. cikk (1) bekezdés e) pontja, **az adatkezelés adatkezelő közérdekű feladatának, valamint közhatalmi jogosítvány gyakorlása körében végzett feladatának végrehajtásához szükséges.**

10. Adatkezelés időtartama, a rögzített felvételek megismerése, továbbítása

Térfelügyelő kamerarendszer képeinek megfigyelése:

A térfelügyelő kamerarendszer által közvetített képek megfigyelésének közvetlen célja, hogy a megfigyelő áttekintést kapjon a megfigyelt közterületek állapotáról, helyzetéről, és indokolt esetben azonnali intézkedést tegyen, illetve kezdeményezzen.

A kamerarendszer által továbbított képek megfigyelésére jogosultak:

- Rendőrség
- Közterület-felügyelő
- Polgárőr

A polgárőr a Pötv.-ben rögzített előírásoknak megfelelően közreműködhet a képfelvevő eszközök által közvetített előképek megfigyelésében, az adatkezelésben további jogosultsága nincsen.

Térfelügyelő kamerarendszer képeinek rögzítése:

A közterületi térfelügyelő kamerarendszer képeinek rögzítése folyamatosan - a nap 24 órájában - történik. A rögzítés célja, hogy szükség esetén bizonyítási eszközként felhasználhatók legyenek az egyes eljárásokban.

A kamerákkal rögzített felvételek – Kfttv-ben rögzített felhasználás hiányában – a rögzítést követő harminc nap elteltével törlésre kerülnek.

Rögzített felvételek visszánézése (betekintés):

A térfelügyelő kamerarendszer rögzített képeinek visszánézésére akkor kerülhet sor, amikor az okot adó esemény - az automatikus törlési határidőn belül - adatkezelő tudomására jut.

A felvételeket kizárólag a Kfttv-ben rögzített célokból használhatók fel:

- a készített felvétel a rögzítés helyszínén elkövetett bűncselekmény vagy szabálysértés miatt indult eljárásban,
- a rögzítés helyszínén elkövetett jogsértés miatt indított közigazgatási hatósági eljárásban,
- a rögzítés helyszínén végzett felügyelői intézkedés jogszerűségének megállapítására irányuló közigazgatási hatósági eljárásban,
- a rögzítés helyszínén a felvételen szereplő személy által, jogainak gyakorlása érdekében indított eljárásban történő felhasználás,
- a terrorcselekmények vagy más bűncselekmények megelőzése, felderítése és megszakítása céljából,
- a nemzetbiztonsági védelmi és elhárítási, információszerzési, továbbá nemzetbiztonsági, iparbiztonsági, belső biztonsági és bűnmegelőzési ellenőrzési feladatok ellátása céljából,
- a katasztrófavédelmi, tűzvédelmi hatósági feladatok ellátása céljából,
- körözött személy vagy tárgy azonosítása érdekében.

A kamerarendszer által továbbított képek visszánézésére jogosultak:

- Rendőrség
- Közterület-felügyelő

A visszánézett felvételeken el kell különíteni a rendkívüli eseményt tartalmazó (azaz a felvételek adatkezelésére indokot, eljárás megindítására, illetve kezdeményezésére okot adó) felvételrészeket a rendkívüli eseményt nem tartalmazó felvételektől.

Biztosítani kell, hogy a felvételen szereplő személy a felvétel törlésének időpontjáig megtekinthesse a róla készült felvételt. Amennyiben ilyen tárgyú kérelem érkezik, a megtekintés előtt meg kell vizsgálni, hogy a kért felvételrészlet rendelkezésre áll-e és azon a kérelmező szerepel-e. Az adatbiztonsági követelmények teljesülése és az érintettek jogainak védelme érdekében adatkezelőnek meg kell győződnie a képfelvételen látható személy és az érintetti jogával élni kívánó személy személyazonosságának egyezéséről, ennek érdekében a felvételekbe történő betekintés az érintett személyes megjelenéséhez kötött.

A felvételen szereplő más érintettek személyes adatai védelméhez fűződő jogai érdekében a felvételen felismerhetően nem szerepelhet más személy vagy személyes adat (pl. rendszám). Szükség esetén ki kell takarni a felvételen szereplőn kívüli személyeket, személyes adatokat.

Eljárás indítása, illetve kezdeményezése:

A rendkívüli eseményt tartalmazó felvételek esetén a felvétel rögzítésétől számított két munkanapon belül a közterület-felügyelő köteles:

- a feladatkörébe tartozó eljárást megindítani, vagy
- a más szerv vagy hatóság (pl. rendőrség) hatáskörébe tartozó eljárások esetén az eljárás megindítását kezdeményezni.

Rögzített felvételek továbbítása:

Az adattovábbítás céljából adatmentést a közterület-felügyelő vagy a rendőrség végezhet.

A rögzített felvétel továbbítható:

- Az eljárásra jogosult szerv, hatóság megkeresésére: a Kftfv-ben rögzített felhasználási célból megkeresésre a rendőrség, a nemzetbiztonsági szolgálat, a hivatásos katasztrófavédelmi szerv részére, illetve bizonyítási eszközként megkeresésre vagy adatkérésre a szabálysértési eljárásra jogosult szerv, illetve büntetőeljárásban a bíróság, az ügyészség, a nyomozó hatóság, az előkészítő eljárást folytató szerv számára, ha a megkeresésben vagy adatkérésben megjelölésre került az eljárás tárgya, ügyszáma és a rögzített felvétellel bizonyítandó tény. A rögzített felvétel továbbítására irányuló megkeresést meg kell tagadni, ha a felvétel a megkeresésben meghatározott tény bizonyítására alkalmatlan.
- A felvételen szereplő személy számára: ha jogainak érvényesítésére eljárást indított, részére az adatkezelési határidőn belül benyújtott kérelemre a felvételt továbbítani kell.
- Akinek jogát vagy jogos érdekét a felvétellel rögzített esemény, cselekmény vagy intézkedés érinti, kérheti, hogy a felvétel ne kerüljön törlésre a felvétel továbbításáig, de legfeljebb a kérelem benyújtását követő harminc napig.

Az eljárásra jogosult szerv, hatóság megkeresésén kívüli esetekben csak a rendkívüli eseményt tartalmazó felvételek továbbítására kerülhet sor, a továbbított felvételen kizárólag a kérelemben szereplő, az eljárás megindítására, illetve kezdeményezésére okot adó kamerafelvétel szerepelhet, biztosítva más érintettek személyes adatai védelméhez fűződő jogait. Szükség esetén ki kell takarni az egyéb személyes adatokat.

A rendszer üzemeltetését, karbantartását végző adatfeldolgozó (személy- és vagyonvédelmi tevékenységet végző alvállalkozó) hatásköre:

A térfigyelő kamerarendszer hardver és szoftverelemeinek karbantartásán kívül kizárólag a Rendőrség vagy a Közterület-felügyelet, mint a kamerarendszer által továbbított képek visszanezésére jogosultak által visszanezett és kimentett, a rendkívüli eseményről készült felvételekkel kapcsolatos technikai műveletekben vehet részt, a szerződésből fakadó kötelezettségei teljesítése céljából, pl. felvételen szereplő személyek, személyes adatok, területek kitakarása, maszkolása. Nem vehet részt a térfigyelő kamerarendszer képeinek megfigyelésében, a rögzített felvételek visszanezésében, továbbításában.

11. Szervezési, technikai és egyéb intézkedések

Az adatkezelő a tudomány és technológia állása és a megvalósítás költségei, 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 érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja. Az adatkezelésében közreműködők a képfelvévő eszközök kezelése során kötelesek betartani azokat a szervezési, technikai és egyéb adatbiztonsági intézkedéseket, amelyek az érintett személy személyes adatait, így különösen magántitkait és magánéletének körülményeit illetéktelen személy tudomására jutásától óvja meg.

Az adatokat védeni kell különösen:

- a jogosulatlan hozzáférés,
- a jogosulatlan megváltoztatás,

- a jogtalan továbbítás,
- a jogtalan nyilvánosságra hozatal,
- jogszerűtlen törlés vagy megsemmisítés, valamint
- a véletlen megsemmisülés és sérülés ellen.

Az adatkezelésben közreműködők a meghatározott feladat ellátása céljából a képfelvételen szereplő személyre vagy járműre vonatkozóan tudomására jutott adatokat, információkat az eredeti céltól eltérően nem használhatják fel, a polgárok a személy- és lakcím, valamint a közúti közlekedési nyilvántartásban tárolt adatok lekérdezésére nem jogosultak.

A kamerarendszer által közvetített képek megfigyelésére, a rögzített felvételek kezelésére csak a hozzáférésre engedélyezett jogosultak, jogosultság nélkül senki sem férhet hozzá személyes adatokhoz, a rendszer a szükséges mértékben naplózza a személyes adatok hozzáféréseit.

A tárolt felvételekhez történő hozzáférés, adattovábbítás dokumentált módon történhet, a jegyzőkönyvnek tartalmaznia kell a rögzített felvétel megismerésének okát és idejét, valamint a megismerő személyét. A 2. melléklet tartalmazza a *Megismerési és adattovábbítási napló* minta dokumentumot.

Az informatikai védelmet az *Adatvédelmi és adatbiztonsági szabályzatban* vagy adatkezelő egyéb szabályzatában, utasításában foglaltaknak megfelelően kell biztosítani.

12. Érintettek jogai

A Rendeletnek és az Infotv-nek megfelelően az érintettek az alábbi főbb jogokat gyakorolhatják:

Előzetes tájékoztatáshoz való jog, hozzáférési jog

A képfeltevő által megfigyelt területre belépő személyek tájékoztatását elősegítő módon figyelemfelhívó jelzést, ismertetést kell elhelyezni a képfeltevők elhelyezéséről, az adatkezelés tényéről.

Adatkezelő a képfeltevők elhelyezésére, a megfigyelt területre vonatkozó adatokat (a kamerák pontos helyszínét, elhelyezését, megfigyelés módját) a település honlapján a Közterület-felügyeletről szóló 1999. évi LXIII. törvény 7. § (4) bekezdése alapján közzéteszi (1. melléklet).

Az érintett magánszemély bármikor jogosult arra, hogy az adatkezeléssel összefüggő tényekről és információkról érthető, tömör tájékoztatást kapjon, ez a joga az adatkezelés megkezdését megelőzően is fennáll. Ezt a célt szolgálja többek között jelen Közterületi térfigyelő kamerarendszer adatkezelési szabályzat, tájékoztató is.

Az érintett jogosult a megadott elérhetőségeken tájékoztatást és hozzáférést (megtekintést, másolatot) kérni az adatkezelő által kezelt személyes adatokról, valamint az adatkezelés jellemzőiről, különösen:

- az adatkezelő és kapcsolattartójának, adatvédelmi tisztviselőjének kilétéről, elérhetőségeiről,
- az adatkezelés céljáról, jogalapjáról, időtartamáról,
- az érintettek jogairól,
- az adatfeldolgozó nevééről, címéről, az adatkezeléssel összefüggő tevékenységéről, amennyiben adatfeldolgozó igénybevétele kerül sor,
- az adattovábbítás jogalapjáról és címzettjéről, amennyiben adattovábbításra kerül sor,
- az esetlegesen bekövetkezett adatvédelmi incidensről (ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az adatkezelő indokolatlan késedelem nélkül tájékoztatja az érintettet az adatvédelmi incidensről).

Adatkezelő a tájékoztatást és intézkedést díjmentesen biztosítja, a betekintést és az adatkezelés tárgyát képező személyes adatok másolatát, a kamerafelvételt az érintett magánszemély erre irányuló kérésére első alkalommal díjmentesen bocsátja rendelkezésére, ezt követően adminisztratív költségeken alapuló, észszerű mértékű díjat számíthat fel.

Ha az érintett kérelme egyértelműen megalapozatlan vagy – különösen ismétlődő jellege miatt – túlzó, figyelemmel a kért információ vagy tájékoztatás nyújtásával vagy a kért intézkedés meghozatalával járó költségekre, díjat számíthat fel vagy megtagadhatja a kérelem alapján történő intézkedést.

A hozzáférési jog, ideértve a másolat rendelkezésre bocsátáshoz való jog feltétel nélkül gyakorolható, az érintettnek nem kell igazolnia a hozzáférési joga gyakorlásához fűződő jogát vagy jogos érdekét, nem kell indokolnia, hogy mi okból kíván élni ezzel a jogával.

A felvételen szereplő személynek a felvétellel kapcsolatos megtekintési, továbbítási jogait a *7. Adatkezelés időtartama, a rögzített felvételek megismerése, továbbítása* pont tartalmazza.

Helyesbítéshez való jog

Az általános adatvédelmi rendelet alapján az érintett jogosult kérelmezni személyes adatainak helyesbítését. Amennyiben adatai megváltoztak, vagy nem pontosak, akkor kérelmére - a személyes adatok kezelésének ideje alatt - bármikor módosítja azokat az adatkezelő.

Törléshez való jog

Az általános adatvédelmi rendelet alapján az érintett élhet a törléshez való jogával, ha adatkezelőre ruházott közhatalmi jogosítványok gyakorlása keretében végzett, vagy közérdekű feladatainak végrehajtásához az adat nem szükséges.

A személyes adatok törlésre kerülnek, ha az adatok kezelése jogellenes, az adatkezelés célja megszűnt, vagy az adatok tárolásának meghatározott határideje lejárt, illetve a bíróság vagy a Nemzeti Adatvédelmi és Információszabadság Hatóság azt jogerősen elrendelte.

Adatkezelés korlátozásához való jog

Adatkezelő korlátozza a személyes adatok kezelését, ha ezt kéri az érintett.

Az érintett a következő esetekben kérheti az adatai korlátozását:

- amennyiben vitatja adatai pontosságát, ez esetben a korlátozás arra az időtartamra vonatkozik, amely lehetővé teszi, hogy az adatkezelő ellenőrizze a személyes adatok pontosságát,
- amennyiben az adatkezelés jogellenes és az érintett ellenzi adatainak törlését és ehelyett kéri azok korlátozását,
- az adatkezelőnek már nincs szüksége a személyes adatokra az adatkezelés céljából, de az érintett igényli azokat jogi igényének előterjesztéséhez, érvényesítéséhez vagy védelméhez,
- az érintett tiltakozik az adatkezelés ellen, ez esetben a korlátozás arra az időtartamra vonatkozik, amíg megállapításra nem kerül, hogy az adatkezelő jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben.

Ha az adatkezelés korlátozás alá esik, a 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. Adatkezelő az érintettet az adatkezelés korlátozásának feloldásáról előzetesen tájékoztatja.

Tiltakozáshoz való jog

Az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból bármikor tiltakozzon személyes adatainak kezelése ellen. Ebben az esetben az adatkezelő a személyes adatokat nem kezelheti tovább, kivéve, ha bizonyítja, hogy az adatkezelést olyan kényszerítő erejű jogos okok indokolják, amelyek elsőbbséget élveznek az érintett érdekeivel, jogaival és szabadságaival szemben, vagy amelyek jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódnak.

Panasz benyújtáshoz vagy jogorvoslathoz való jog

Az érintettnek jogai sérelme esetén célszerű egyeztetést kezdeményeznie az adatkezelő képviselőjével a megadott elérhetőségeken. Amennyiben ez nem vezet eredményre, vagy nem kívánja, jogosult bírósághoz vagy panasszal a Nemzeti Adatvédelmi és Információszabadság Hatósághoz (NAIH) fordulni.

Bírósági eljárás kezdeményezése esetén a bíróság soron kívül jár el. Dönthet úgy, hogy a pert a lakóhelye vagy tartózkodási helye szerinti törvényszék előtt indítja meg.

NAIH elérhetőségei:

1125 Budapest, Szilágyi Erzsébet fasor 22/C, Postacím: 1530 Budapest, Pf.: 5.

Telefonszám: +36 1 3911400; fax: +36 1 3911410; e-mail: ugyfelszolgalat@naih.hu; honlap: naih.hu

Bővebb tájékoztatást az *Adatvédelmi és adatbiztonsági szabályzat* tartalmaz.

Verzió: v1.02

Képfeltevők elhelyezése, a megfigyelt területre vonatkozó adatok

kamera típus jelmagyarázat:

D = Dome (360°-ban forgatható, pásztázó)

F = Fix

R = rendszámfelismerő

sorszám	kamera típus	telepítési hely, megfigyelt közterület
01	D	Kereszteződés; Miskolci u. – Malom u. – II. Rákóczi F. u. kereszteződés
02	F	Kassai u.; Petőfi S. u. – Kassai u. kereszteződés
03	F	Miskolci u.; Miskolc felől bevezető szakasz
04	F	Bajcsy-Zsilinszky E. u.; Alsóvadász felé vezető szakasz
05	F	Mátyás király u.; Nagyállomás felé vezető szakasz
06	F	Vasút u.; Kisállomás felé vezető szakasz
07	F	Lőcsei u.; Dózsa Gy. u. – Lőcsei u. kereszteződés + II. Rákóczi F. u. – Dózsa Gy. u. kereszteződés
08	F	Bethlen G. u.; Bethlen G. u. Piac tér felőli vége
09	F	Szádellői u.; Zsidó temető felé
10	F	Petőfi S. u.; Balogh A. tér.
11	F	Kálvin tér 1. (Református parókia); Táncsics u. Kossuth L. u. felé
12	F	Kálvin tér 2. (Református parókia); Táncsics u. Egészség ház felé
13	F	Malom u. – Bethlen G. u. kereszteződés; Malom u. Sportcsarnok előtti szakasz
14	F	Bártfai u.; Bártfai u. Gömöri Tanműhely felé
15	F	Szőlőhegy
16	F	Borok háza; Borok házatól levezető útszakasz
17	F	Kazinczy F. u.; Temető hátsó bejárata
18	F	Arany J. u.; Arany J. u. – Alibég u. kereszteződés
19	F	Radnóti M. u.; Deák F. u. – Radnóti M. u.

.....
dátum

.....
Sváb Antal Béla



Szikszó Város Önkormányzata
3800 Szikszó, Kálvin tér 1.
Tel:(46) 596-450; Fax:(46) 596-211
info@szikszo.hu

HATÁROZAT

18/2020.(V.29.) Szikszó Város Önkormányzat Polgármesteri Határozata

Szikszó Város Önkormányzat Polgármestere a veszélyhelyzet kihirdetéséről szóló 40/2020. (III.11.) számú kormányrendelet, valamint a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény 46.§ (4) bekezdésében foglalt jogköre alapján a Képviselő-testület feladat- és hatáskörében eljárva az alábbiak szerint határoz:

Döntés a Szikszói Közös Önkormányzati Hivatal Adatvédelmi és adatbiztonsági szabályzatának elfogadásáról

Szikszó Város Önkormányzat Polgármestere úgy határoz, hogy 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 (EU) 2016/679 rendelet (Általános adatvédelmi rendelet vagy GDPR) és az Információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény alapján elfogadja a határozat mellékletét képező „Adatvédelmi és adatbiztonsági szabályzat”-ot Szikszói Közös Önkormányzati Hivatalra vonatkozóan.
(Írásos anyag csatolva: 5. sz. melléklet)

Felelős: polgármester
Határidő: azonnal

Kelt: Szikszó, 2020.05.29.





Szikszói Közös Önkormányzati Hivatal

3800 Szikszó, Kálvin tér 1.

ADATVÉDELMI ÉS ADATBIZTONSÁGI SZABÁLYZAT

Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.)
a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről
és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről
(általános adatvédelmi rendelet) szerint

érvényes:

2020.05.29

jóváhagyta:

Battány

Battáné dr. Tóth Zita



Tartalomjegyzék

Vezetői nyilatkozat.....	4
Adatkezelő/adatfeldolgozó adatai	5
1. A személyes adatok kezelésére vonatkozó általános elvek	6
1.0. Áttekintés az Európai Parlament és a Tanács (EU) 2016/679 rendeletéről	6
1.1. Az Adatvédelmi és adatbiztonsági szabályzat célja	6
1.2. Az Adatvédelmi és adatbiztonsági szabályzat hatálya	7
1.3. Kapcsolódó jogforrások, egyéb szabályzatok	7
1.4. A személyes adatok kezelésére vonatkozó elvek	8
1.5. Az adatkezelés jogszerűsége	9
1.6. Különleges adatok (a személyes adatok különleges kategóriáinak) kezelése.....	9
1.7. Bizonyítható hozzájárulás.....	10
1.8. Az érintett jogai	11
1.9. Felelősségi körök, Szervezet vezetőjének feladatai.....	13
1.10. Adatvédelmi tisztviselő.....	14
1.11. Képzés.....	14
2. A szervezet adatvédelmi feladatai	15
2.1. Adatvédelmi tisztviselő kijelölése	15
2.2. Adatkezelési, adatfeldolgozói tevékenységek nyilvántartása	16
2.3. Átlátható tájékoztatás, kommunikáció és az érintett jogainak gyakorlására vonatkozó intézkedések.....	17
2.3.1. Tájékoztatás és a személyes adatokhoz való hozzáférés joga.....	18
2.3.2. Az érintett hozzáférési joga.....	19
2.3.3. Az érintett helyesbítéshez való joga	20
2.3.4. A törléshez, elfeledtetéshez való jog	20
2.3.5. Az adatkezelés korlátozásához való jog	21
2.3.6. A személyes adatok helyesbítéséhez vagy törléséhez, illetve az adatkezelés korlátozásához kapcsolódó értesítési kötelezettség	22
2.3.7. Az adathordozhatósághoz való jog.....	22
2.3.8. A tiltakozáshoz való jog	22
2.3.9. Automatizált döntéshozatal egyedi ügyekben, profilalkotás.....	22
2.3.10. A személyes adatokkal összefüggő jogok érvényesítése az érintett halálát követően.....	23
2.4. Az érintetti kérelmek kezelése	23
2.5. Az adatkezelés biztonsága, technikai és szervezési intézkedések végrehajtása	24
2.6. Az adatvédelmi incidensek.....	25
2.6.1. Incidensek belső nyilvántartása.....	25
2.6.2. Incidens NAIH bejelentése	25
2.6.3. Érintettek tájékoztatása az Incidensről.....	26
2.6.4. Adatvédelmi incidensek kezelése	26
2.7. Érdemérlegelés	27
2.8. Adatközlés, adattovábbítás, nyilvánosságra hozatal.....	28
2.8.1. Adattovábbítás harmadik országokba	28
2.9. Adatfeldolgozás, adatfeldolgozói garancianyújtás.....	29
2.10. Kötelező adatkezelések felülvizsgálata.....	31
2.11. Adatvédelmi hatásvizsgálat.....	32
3. Személyes adatok kezelése, nyilvántartása	33
3.1. Munkavállalók adatkezelései	33
3.2. Ügyfelekkel, szakfeladatokkal kapcsolatos adatkezelések	35

3.2.1.	Okmánymásolás	36
4.	Technikai és szervezési intézkedések	37
4.1.	Adminisztratív védelmi intézkedések	37
4.2.	Fizikai védelmi intézkedések	40
4.3.	Logikai védelmi intézkedések	41
4.4.	Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény hatálya alá tartozó szervek további követelményei	45
Fogalomtár	46

Verzió: v1.01

Vezetőinyilatkozat

A Szikszói Közös Önkormányzati Hivatal (továbbiakban Szervezet) vezetőjeként hatályba léptetem jelen Adatvédelmi és adatbiztonsági szabályzatot, annak érdekében, hogy a Szervezet alkalmazza az Európai Parlament és a Tanács (EU) 2016/679 rendeletét (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 (továbbiakban Rendelet) előírásait, figyelembe véve az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény 2. § (2) bekezdése alapján vonatkozó rendelkezéseit.

A Szikszói Közös Önkormányzati Hivatal vezetője megismerve a GDPR által támasztott kihívásokat, elkötelezett aziránt, hogy a Szervezet az adatvédelmi szabályoknak megfeleljen, felelős jelen Adatvédelmi és adatbiztonsági szabályzat folyamatos karbantartásáért és az abban foglaltak végrehajtásáért.

A szabályzat a GDPR előírásait követve, a Szervezet minden telephelyén, szervezeti egységén, munkaterületén, minden tevékenységére rögzíti a személyes adatok kezelésére vonatkozó előírásokat, eljárásokat, és egyértelműen meghatározza a kapcsolódó dokumentált információs rendszert.

A Szervezet biztosítja a Rendelet és jelen szabályzat elvárásainak teljesítéséhez szükséges anyagi és személyi erőforrásokat.

2020.05.29



Adatkezelő/adatfeldolgozó adatai

Adatkezelő, adatfeldolgozó neve: Szikszói Közös Önkormányzati Hivatal

Címe (hivatalos levelezési cím): 3800 Szikszó, Kálvin tér 1.

Honlapjának elérhetősége: <https://www.szikszo.hu>

Telefonszáma: +36 46 596444

Adószáma: 15810908-2-05

Képviselője neve: Battáné dr. Tóth Zita

Adatkezelési tájékoztató elérhetősége: 3800 Szikszó, Kálvin tér 1.

Adatvédelmi tisztviselő neve: Juhász Gergely

Adatvédelmi tisztviselő elérhetősége: adatvedelem@szikszo.hu

Nyilatkozat Adatvédelmi tisztviselő kijelöléséről:

Adatvédelmi tisztviselő kijelölésére kerül sor, mert:

- Az adatkezelést közhatalmi szervek vagy egyéb, közfeladatot ellátó szervek végzik, kivéve az igazságszolgáltatási feladatkörükben eljáró bíróságokat

1. A személyes adatok kezelésére vonatkozó általános elvek

1.0. Áttekintés az Európai Parlament és a Tanács (EU) 2016/679 rendeletéről

2016. május 25-én lépett hatályba és 2018. május 25-től kötelezően alkalmazandó az Európai Unió valamennyi tagállamában az új európai adatvédelmi rendelet (az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet, Rendelet). A Rendelet a természetes személyeknek a személyes adatok kezelése tekintetében történő védelmére és a személyes adatok szabad áramlására vonatkozó szabályokat állapít meg.

A rendeletet kell alkalmazni a személyes adatoknak az Unióban tevékenységi hellyel rendelkező adatkezelők vagy adatfeldolgozók tevékenységeivel összefüggésben végzett kezelésére, függetlenül attól, hogy az adatkezelés az Unió területén történik vagy nem, valamint ha az adatkezelés az Unióban tartózkodó érintettek személyes adatainak kezelésre irányul, akkor is, ha az Unióban az adatkezelő vagy az adatfeldolgozó tevékenységi hellyel nem rendelkezik.

1.1. Az Adatvédelmi és adatbiztonsági szabályzat célja

Az adatkezelőnek, adatfeldolgozónak belső adatvédelmi szabályokat kell alkalmaznia a személyes adatok védelmének biztosítása céljából megvalósított technikai és szervezési intézkedések részeként, ha ez az adatkezelési tevékenység vonatkozásában arányos.

A közfeladatot ellátó szerv az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Infotv.) szerinti kötelezően közzéteendő közérdekű adatok közzétételi kötelezettségét jelen szabályzat hatályos és teljes szövegének közzétételével teljesíti.

Jelen szabályzat célja a hatálya alá tartozó tárgykörökben az adatok kezelésére vonatkozó alapvető szabályok meghatározása annak érdekében, hogy a természetes személyek magánszféráját az adatkezelő, munkavállalói vagy egyéb, munkavégzésre irányuló jogviszony alapján foglalkoztatott személyek, illetőleg a szerződéses kapcsolatban álló partnerek vagy más harmadik természetes személyek által tiszteletben tartásuk, minden adatkezelési folyamat, munkavégzés, közfeladat teljesítése során a meghatározott adatkezelési célból, a szervezet részére átadott személyes adataik kezelése, továbbítása, feldolgozása, tárolása során biztosítva legyen az adatalanyok információs önrendelkezési jogának maradéktalan érvényesülése, törvényes érdekeik és jogaik védelme, az adatok kezelésének jogszerű célhoz rendelése és a felhasználás alatt mindvégig e célhoz kötöttsége.

Az Adatvédelmi és adatbiztonsági szabályzat további célja, hogy meghatározza a működés során az adatkezeléssel kapcsolatos nyilvántartások vezetésének törvényes rendjét, biztosítsa az adatvédelem alkotmányos elveinek, az információs önrendelkezési jognak az érvényesülését, valamint hogy a személyes adatok kezelése a jogszabályokban előírtaknak megfelelően történjen.

Az adatalanyi minőség - és ezáltal az adatvédelmi szabályoknak történő megfelelés követelménye - a személyes adat jogszerű módon történő megszerzésétől kezdődően, az adott jogviszony létrehozásán keresztül annak fennállása alatt és azt követően is fennáll mindaddig, amíg az adott adatalanyal összefüggésben a személyes adatok végleges és visszafordíthatatlan módon történő törlése - vagy ahol az lehetséges, illetve szükséges, a megsemmisítése - végrehajtásra nem kerül.

1.2. Az Adatvédelmi és adatbiztonsági szabályzat hatálya

A Szikszói Közös Önkormányzati Hivatal(továbbiakban Szervezet) jelen Adatvédelmi és adatbiztonsági szabályzatának hatálya valamennyi olyan szervezeti egységére, telephelyére kiterjed, amely részt vesz a keletkezett, feldolgozott, tárolt, illetve továbbított személyes adatok kezelésében, valamennyi munkatársra, munkavégzésre irányuló jogviszony alapján foglalkoztatott személyre, szerződéses kapcsolatban álló partnerre, akik a szervezet által használt rendszerekhez és az azokban tárolt személyes adatokhoz hozzáféréssel rendelkeznek, illetve akik részt vesznek a szervezetnél keletkezett, feldolgozott, tárolt, illetve továbbított személyes adatok kezelésében.

A szerződéses partnerekkel, harmadik felekkel szembeni elvárásokat, kötelezettségeket a tevékenységet képező, jogviszonyt megalapozó szerződésekben, megállapodásokban kell érvényesíteni. Meg kell ismertetni a szerződéses partnerekkel, harmadik felekkel az adatkezelésre, titoktartási kötelezettségekre vonatkozó felételeket.

Egyéni vállalkozó, egyéni cég, őstermelő magánszemély e szabályzat alkalmazásában természetes személynek minősül, így adataik kezelése kapcsán személyes adatkezelés történik.

Aszabályzat a kiadás napján lép hatályba, mellyel a korábbi ezzel kapcsolatos szabályzat hatályát veszti.

A Szabályzatot az adatkezelések körülményeiben beállt lényeges változások esetén, de legalább 3 évenként felül kell vizsgálni

1.3. Kapcsolódó jogforrások, egyéb szabályzatok

- Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (a továbbiakban: Rendelet)
- Magyarország Alaptörvénye (2011. április 25.)
- 2011. évi CXII. törvény az információs önrendelkezési jogról és információszabadságról (Infotv.),
- 2013 évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (Ibtv.)
- 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről
- 2005. évi CXXXIII. törvény a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól (Szvtv.)
- 1999. évi LXIII. törvény a közterület-felügyeletről (Kftfv.)
- 2011. évi CLXV. törvény a polgárőrségről és a polgárőri tevékenység szabályairól
- 1994. évi XXXIV. törvény a Rendőrségről (Rtv.)
- 2012. évi I. törvény a munka törvénykönyvéről (Mt.)
- 2011. évi CXCV. törvény a közszolgálati tisztviselőkről (Ktv.)
- 1992. évi XXXIII. törvény a közalkalmazottak jogállásáról
- 2013. évi V. törvény a polgári törvénykönyvről (Ptk.)
- 2011. évi CXCV. törvény az államháztartásról
- 2011. évi CLXXXIX. törvény Magyarország helyi önkormányzatairól
- 1991. évi XX. törvény a helyi szervezet, intézmények és szerveik, a köztársasági megbízottak, valamint egyes centrális alárendeltségű szervek feladat- és hatásköreiről

- 2017. évi I. törvény a közigazgatási perrendtartásról
- 1995. évi CXVII. törvény a személyi jövedelemadóról (Szja.)
- 2017. évi CL. törvény az adózás rendjéről (Art.)
- 1997. évi LXXXI. törvény a társadalombiztosítási nyugellátásról
- 2000. évi C. törvény a számvitelről (Sztv.)
- 2017. évi LIII. törvény a pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról (Pmt.)
- NAIH ajánlások: <https://www.naih.hu/ajanlasok.html>
- 29-Adatvédelmi Munkacsoport dokumentumai: <https://naih.hu/29--adatvedelmi-munkacsoport-dokumentumai.html>
- **Kapcsolódó főbb belső szabályzatok:**
 - Informatikai biztonsági szabályzat (az lbtv. hatálya alá tartozó szervezeteknek, többek között a helyi és a nemzetiségi önkormányzatok képviselő-testületének hivatalainak, a hatósági igazgatási társulásoknak, valamint ezen szervek számára adatkezelést végzőknek)
 - Közszolgálati szabályzat (Ktv. hatálya alá tartozó szervezeteknek)

1.4. A személyes adatok kezelésére vonatkozó elvek

1. **Jogszerűség, tisztességes eljárás és átláthatóság:** A személyes adatok kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni.
2. **Célhoz kötöttség:** A személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történjen, és azokat ne kezeljék ezekkel a célokkal össze nem egyeztethető módon. Nem minősül az eredeti céllal össze nem egyeztethetőnek a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból történő további adatkezelés.
3. **Adattakarékosság:** A személyes adatok az adatkezelés céljai szempontjából megfelelőek és relevánsak kell, hogy legyenek, és a szükségesre kell korlátozódniuk.
4. **Pontosság:** A személyes adatoknak pontosnak és szükség esetén naprakésznek kell lenniük. Minden ésszerű intézkedést meg kell tenni annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul töröljék, vagy helyesbítsék.
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 kezelésére közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból kerül majd sor, az érintettek jogainak és szabadságainak védelme érdekében előírt megfelelő technikai és szervezési intézkedések végrehajtására is figyelemmel.
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.
7. **Elszámoltathatóság:** Az adatkezelő felelős a fenti alapelveknek való megfelelésért, továbbá képesnek kell lennie e megfelelés igazolására.

1.5. Az adatkezelés jogszerűsége

A Rendelet hat lehetséges jogalapot tartalmaz azon személyes adatok kezelése tekintetében, amelyek nem tartoznak a személyes adatok különleges kategóriájába (pl. egészségügyi, biometrikus vagy genetikai adatok).

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.

1.6. Különleges adatok (a személyes adatok különleges kategóriáinak) kezelése

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 kezelése tilos, a különleges adatok kezelése csak a felsorolt esetekben lehetséges:

- a) az érintett kifejezett hozzájárulását adta az említett személyes adatok egy vagy több konkrét célból történő kezeléséhez, kivéve, ha az uniós vagy tagállami jog úgy rendelkezik, hogy a tilalom nem oldható fel az érintett hozzájárulásával;
- b) az adatkezelés az adatkezelőnek vagy az érintettnek a foglalkoztatást, valamint a szociális biztonságot és szociális védelmet szabályozó jogi előírásokból fakadó kötelezettségei teljesítése és konkrét jogai gyakorlása érdekében szükséges, ha az érintett alapvető jogait és érdekeit védő megfelelő garanciákról is rendelkező uniós vagy tagállami jog, illetve a tagállami jog szerinti kollektív szerződés ezt lehetővé teszi;
- c) az adatkezelés az érintett vagy más természetes személy létfontosságú érdekeinek védelméhez szükséges, ha az érintett fizikai vagy jogi cselekvőképtelensége folytán nem képes a hozzájárulását megadni;
- d) az adatkezelés valamely politikai, világnézeti, vallási vagy szakszervezeti célú alapítvány, egyesület vagy bármely más nonprofit szervezet megfelelő garanciák mellett végzett jogszerű tevékenysége keretében történik, azzal a feltétellel, hogy az adatkezelés kizárólag az ilyen szerv jelenlegi vagy volt tagjaira, vagy olyan személyekre vonatkozik, akik a szervezettel rendszeres kapcsolatban állnak a szervezet céljaihoz kapcsolódóan, és hogy a személyes adatokat az érintettek hozzájárulása nélkül nem teszik hozzáférhetővé a szervezeten kívüli személyek számára;

- e) az adatkezelés olyan személyes adatokra vonatkozik, amelyeket az érintett kifejezetten nyilvánosságra hozott;
- f) az adatkezelés jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez szükséges, vagy amikor a bíróságok igazságszolgáltatási feladatkörükben járnak el;
- g) az adatkezelés jelentős közérdek miatt szükséges, uniós jog vagy tagállami jog alapján, amely arányos az elérni kívánt céllal, tiszteletben tartja a személyes adatok védelméhez való jog lényeges tartalmát, és az érintett alapvető jogainak és érdekeinek biztosítására megfelelő és konkrét intézkedéseket ír elő;
- h) az adatkezelés megelőző egészségügyi vagy munkahelyi egészségügyi célokból, a munkavállaló munkavégzési képességének felmérése, orvosi diagnózis felállítása, egészségügyi vagy szociális ellátás vagy kezelés nyújtása, illetve egészségügyi vagy szociális rendszerek és szolgáltatások irányítása érdekében szükséges, uniós vagy tagállami jog alapján vagy egészségügyi szakemberrel kötött szerződés értelmében (ha ezen adatok kezelése olyan szakember által vagy olyan szakember felelőssége mellett történik, aki uniós vagy tagállami jogban, illetve az arra hatáskörrel rendelkező tagállami szervek által megállapított szabályokban meghatározott szakmai titoktartási kötelezettség hatálya alatt áll, illetve olyan más személy által, aki szintén uniós vagy tagállami jogban, illetve az arra hatáskörrel rendelkező tagállami szervek által megállapított szabályokban meghatározott titoktartási kötelezettség hatálya alatt áll);
- i) az adatkezelés a népegészségügy területét érintő olyan közérdekből szükséges, mint a határokon át terjedő súlyos egészségügyi veszélyekkel szembeni védelem vagy az egészségügyi ellátás, a gyógyszerek és az orvostechikai eszközök magas színvonalának és biztonságának a biztosítása, és olyan uniós vagy tagállami jog alapján történik, amely megfelelő és konkrét intézkedésekről rendelkezik az érintett jogait és szabadságait védő garanciákra, és különösen a szakmai titoktartásra vonatkozóan;
- j) az adatkezelés a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból szükséges olyan uniós vagy tagállami jog alapján, amely arányos az elérni kívánt céllal, tiszteletben tartja a személyes adatok védelméhez való jog lényeges tartalmát, és az érintett alapvető jogainak és érdekeinek biztosítására megfelelő és konkrét intézkedéseket ír elő.

A tagállami jog különös rendelkezéseket állapíthat meg az adatok védelmére vonatkozóan annak érdekében, hogy kiigazítsák a Rendeletben foglalt szabályok alkalmazását valamely jogi kötelezettségnek való megfelelés vagy közérdekből végzett feladat végrehajtása vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlása tekintetében.

1.7. Bizonyítható hozzájárulás

Ha az adatkezelés az érintett hozzájárulásán alapul, az adatkezelőnek kell tudni bizonyítania, hogy az adatkezelési művelethez az érintett hozzájárult. A hozzájárulás önkéntességének megállapításához figyelembe kell venni többek között azt a ténytet, hogy a szerződés teljesítésének – beleértve a szolgáltatások nyújtását is – feltételül szabták-e az olyan személyes adatok kezeléséhez való hozzájárulást, amelyek nem szükségesek a szerződés teljesítéséhez.

Különösen a más ügyben tett írásbeli nyilatkozattal összefüggésben garanciákkal szükséges biztosítani azt, hogy az érintett tisztában legyen azzal a ténnyel, hogy hozzájárulását adta, valamint azzal, hogy ezt milyen mértékben tette. Egy hozzájárulás egy adatkezelési cél érdekében végzett adatkezeléshez való hozzájárulást jelenti. Az adatkezelő lehetőség szerint előre megfogalmazott hozzájárulási nyilatkozatról

gondoskodik, amelyet érthető és könnyen hozzáférhető formában bocsát rendelkezésre, nyelvezetének, pedig világosnak és egyszerűnek kell lennie, és nem tartalmazhat tisztességtelen feltételeket.

Ahhoz, hogy a hozzájárulás tájékoztatáson alapuljon, az érintettnek legalább tisztában kell lennie az adatkezelő kilétével és a személyes adatok kezelésének céljával.

A hozzájárulás megadása nem tekinthető önkéntesnek, ha az érintett nem rendelkezik valós vagy szabad választási lehetőséggel, és nem áll módjában a hozzájárulás nélküli megtagadása vagy visszavonása, hogy ez kárára válna.

Az érintett jogosult arra, hogy hozzájárulását bármikor visszavonja. A visszavonás nem érinti a hozzájáruláson alapuló, a visszavonás előtti adatkezelés jogszerűségét. A hozzájárulás visszavonását ugyanolyan egyszerű módon kell lehetővé tenni, mint annak megadását.

Hozzájárulásra, mint jogalapra, a munkahelyi adatkezelések esetében csak kivételesen lehet hivatkozni a munkáltató és a munkavállaló között fennálló függelmi jelleg miatt.

A Szikszói Közös Önkormányzati Hivataladatkezeléseihez kapcsolódóan a hozzájárulás alapú adatkezelések esetén a GDPR Reg Adatkezelési rendszerben is generálhat szerkeszthető hozzájáruló nyilatkozatot, mely tartalmazza a kiválasztott adatkezelésekre vonatkozóan az érintettek tájékoztatására szolgáló valamennyi adatot, információt.

1.8. Az érintett jogai

A Rendeletnek és az Infotv-nek megfelelően az érintettek az alábbi főbb jogokat gyakorolhatják:

- Előzetes tájékoztatáshoz való jog:** Az érintett magánszemély bármikor jogosult arra, hogy az adatkezeléssel összefüggő tényekről és információkról érthető, tömör tájékoztatást kapjon, ez a joga az adatkezelés megkezdését megelőzően is fennáll.
- A hozzáférésjoga:** Az érintett jogosult arra, hogy az adatkezelőtől tömör, közérthető visszajelzést kapjon arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e, és ha ilyen adatkezelés folyamatban van, jogosult arra, hogy a személyes adatokhoz és a Rendeletben felsorolt információkhoz hozzáférést kapjon.
- A helyesbítéshez való jog:** Az érintett jogosult arra, hogy kérésére az adatkezelő indokolatlan késedelem nélkül helyesbítse a rá vonatkozó pontatlan személyes adatokat. Figyelembe véve az adatkezelés célját, az érintett jogosult arra, hogy kérje a téves, hibás, hiányos személyes adatok – egyebek mellett kiegészítő nyilatkozat útján történő – módosítását, kiegészítését.
- A törléshez való jog:** Az érintett jogosult arra, hogy kérésére az adatkezelő indokolatlan késedelem nélkül törölje a rá vonatkozó személyes adatokat, az adatkezelő pedig köteles arra, hogy az érintettre vonatkozó személyes adatokat indokolatlan késedelem nélkül törölje meghatározott feltételek esetén (ha annak nincs jogi akadálya). Az érintettnek ez a joga különösen a hozzájárulása alapján kezelt személyes adataihoz kapcsolódóan áll fent, más jogalapok fennállta, így többek között a jogi kötelezettség teljesítése alapján kezelt adatok esetén pedig kifejezetten korlátozott ez a joga, illetve nem áll fent.
- Az elfeledtetéshez való jog:** Ha az adatkezelő nyilvánosságra hozta a személyes adatot, és azt törölni köteles, az elérhető technológia és a megvalósítás költségeinek figyelembevételével megteszi az észszerűen elvárható lépéseket – ideértve technikai intézkedéseket – annak érdekében, hogy tájékoztassa az adatokat kezelő adatkezelőket, hogy az érintett kérelmezte tőlük a szóban forgó személyes adatokra mutató linkek vagy e személyes adatok másolatának, illetve másodpéldányának törlését.

6. **Az adatkezelés korlátozásához való jog:** Az érintett jogosult arra, hogy kérésére az adatkezelő korlátozza az adatkezelést, ha az alábbi feltételek valamelyike teljesül:
- az érintett vitatja a személyes adatok pontosságát, ez esetben a korlátozás arra az időtartamra vonatkozik, amely lehetővé teszi, hogy az adatkezelő ellenőrizze a személyes adatok pontosságát,
 - az adatkezelés jogellenes, és az érintett ellenzi az adatok törlését, és e helyett kéri azok felhasználásának korlátozását,
 - az adatkezelőnek már nincs szüksége a személyes adatokra adatkezelés céljából, de az érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez, vagy védelméhez,
 - az érintett tiltakozott az adatkezelés ellen; ez esetben a korlátozás arra az időtartamra vonatkozik, amíg megállapításra nem kerül, hogy az adatkezelő jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben.
7. **A személyes adatok helyesbítéséhez vagy törléséhez, illetve az adatkezelés korlátozásához kapcsolódó értesítési kötelezettség:** Az adatkezelő minden olyan címzettet tájékoztat minden helyesbítésről, törlésről vagy adatkezelés-korlátozásról, akikkel a személyes adatot közölték. Kivétel: nem várható el ezen kötelezettség teljesítése, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényelne.
8. **Az adathordozhatósághoz való jog:** Az érintett jogosult arra, hogy a rá vonatkozó, általa egy adatkezelő rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja és jogosult arra, hogy ezeket az adatokat egy másik adatkezelőnek továbbítsa anélkül, hogy ezt akadályozná az az adatkezelő, amelynek a személyes adatokat a rendelkezésére bocsátotta.
9. **A tiltakozáshoz való jog:** Az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból bármikor tiltakozzon személyes adatainak a kezelése ellen (ideértve a profilalkotást is):
- ha az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához, illetve az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges (tiltakozás esetén a személyes adatok nem kezelhetők tovább, kivéve, ha az adatkezelő bizonyítja, hogy az adatkezelést olyan kényszerítő erejű jogos okok indokolják, amelyek elsőbbséget élveznek az érintett érdekeivel, jogaival és szabadságaival szemben, vagy amelyek jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódnak).
 - közvetlen üzletszerzés esetén: ha az érintett tiltakozik a személyes adatok közvetlen üzletszerzés érdekében történő kezelése ellen, akkor a személyes adatok a továbbiakban e célból nem kezelhetők.
10. **Automatizált döntéshozatal egyedi ügyekben, beleértve a profilalkotást:** Az érintett jogosult arra, hogy ne terjedjen ki rá az olyan, kizárólag automatizált adatkezelésen – ideértve a profilalkotást is – alapuló döntés hatálya, amely rá nézve joghatással járna vagy őt jelentős mértékben érintené (kivéve ha az adatkezelés az érintett és az adatkezelő közötti szerződés megkötése vagy teljesítése érdekében szükséges, vagy meghozatalát az adatkezelőre alkalmazandó olyan uniós vagy tagállami jog teszi lehetővé, amely az érintett jogainak és szabadságainak, valamint jogos érdekeinek védelmét szolgáló megfelelő intézkedéseket is megállapít, vagy az érintett kifejezett hozzájárulásán alapul).
11. **Az érintett tájékoztatása az adatvédelmi incidensről:** Adatkezelőnek indokolatlan késedelem nélkül tájékoztatnia kell az érintettet – ismertetve vele az Adatvédelmi tisztviselőt vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit, valamint az adatvédelmi incidensből eredő,

valószínűsíthető következményeket –, ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár jogaira és szabadságaira nézve, kivéve ha:

- adatkezelő megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre, melyeket az incidens által érintett adatok tekintetében alkalmaztak (pl. a titkosítás, amely a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné tesz az adatokat),
- 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,
- a tájékoztatás aránytalan erőfeszítést tenne szükségessé - ilyen esetekben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, vagy olyan hasonló intézkedést kell hozni, amely biztosítja az érintettek hasonlóan hatékony tájékoztatását.

- 12. A felügyeleti hatóságnál történő panasztételhez való jog** (hatósághoz való fordulás joga): Az érintett magánszemély jogosult arra, hogy panaszt tegyen egy felügyeleti hatóságnál – különösen a szokásos tartózkodási helye, a munkahelye vagy a feltételezett jogsértés helye szerinti tagállamban –, ha az érintett megítélése szerint a rá vonatkozó személyes adatok kezelése megsérti az uniós adatvédelmi rendeletet.
- 13. A felügyeleti hatósággal szembeni hatékony bírósági jogorvoslathoz való jog:** Minden természetes és jogi személy jogosult a hatékony bírósági jogorvoslatra a felügyeleti hatóság rá vonatkozó, jogilag kötelező erejű döntésével szemben. Ez a jog akkor is fennáll, ha a felügyeleti hatóság nem foglalkozik a panasszal, vagy három hónapon belül nem tájékoztatja az érintettet a benyújtott panasszal kapcsolatos eljárási fejleményekről vagy annak eredményéről.
- 14. Az adatkezelővel vagy az adatfeldolgozóval szembeni hatékony bírósági jogorvoslathoz való jog:** Minden érintett hatékony bírósági jogorvoslatra jogosult, ha megítélése szerint a személyes adatainak az uniós rendeletnek nem megfelelő kezelése következtében megsértették a jogait. Az bírósági illetékességi szabályok szerinti Törvényszék jogosult az eljárásra.
- 15. A személyes adatokkal összefüggő jogok érvényesítése az érintett halálát követően:** Az Infotv. szerint az érintett halálát követő öt éven belül a Rendelet hatálya alá tartozó adatkezelési műveletek esetén az elhaltat életében megillető jogokat az érintett által arra ügyintézési rendelkezéssel, illetve közokiratban vagy teljes bizonyító erejű magánokiratban foglalt, az adatkezelőnél tett nyilatkozattal - ha az érintett egy adatkezelőnél több nyilatkozatot tett, a későbbi időpontban tett nyilatkozattal - meghatalmazott személy jogosult érvényesíteni. Ha az érintett nem tett megfelelő jognyilatkozatot, a Ptk. szerinti közeli hozzátartozója annak hiányában is jogosult az elhaltat életében megillető jogokat érvényesíteni az érintett halálát követő öt éven belül. Az érintett jogainak érvényesítésére az a közeli hozzátartozó jogosult, aki ezen jogosultságát elsőként gyakorolja.

1.9. Felelősségi körök, Szervezet vezetőjének feladatai

A Szikszói Közös Önkormányzati Hivatal vezetője (továbbiakban vezető) felelős azért, hogy az általa vezetett Szervezet az adatkezelési, adatfeldolgozási tevékenységét úgy végezze, hogy megfeleljen a Rendeletnek, amely szabályozza a természetes személyeknek a személyes adatok kezelése tekintetében történő védelmét és az ilyen adatok szabad áramlását, és biztosítja az érintettek számára a jogi garanciákat. Felelős azért, hogy az adatkezelési tevékenységek során betartsa a személyes adatok kezelésére vonatkozó elveket, és képes e megfelelések igazolására („elszámoltathatóság”).

Felelős azért, hogy:

- A személyes adatoknak bármilyen jellegű kezelése tekintetében az adatkezeléssel kapcsolatos hatásköröket és felelősségét egyértelműen meghatározza, szabályozza.
- Megfelelő és hatékony intézkedéseket hajtson végre, valamint képes legyen igazolni azt, hogy az adatkezelési tevékenységek a Rendeletnek megfelelnek, és az alkalmazott intézkedések hatékonysága is a Rendelet által előírt szintű. Az intézkedéseket az adatkezelés jellegének, hatókörének, körülményeinek és céljainak, valamint a természetes személyek jogait és szabadságait érintő kockázatnak a figyelembevételével kell meghozni.
- Megteremtse a szervezet informatikai rendszereinek és a benne kezelt adatoknak a biztonságát, meghatározza és biztosítsa a szervezet informatikai biztonsági követelményrendszerét és környezetét, az elektronikus információs rendszereivel kapcsolatba kerülő személyek felé támasztott követelményeket, elvárásokat, kötelezettségeket és a felelősséget.
- Olyan adatfeldolgozókat vegyen igénybe, amelyek megfelelő garanciákat nyújtanak – különösen a szakértelem, a megbízhatóság és az erőforrások tekintetében – arra vonatkozóan, hogy az a rendelet követelményeinek teljesülését biztosító technikai és szervezési intézkedéseket végrehajtják, ideértve az adatkezelés biztonságát is.
- A Rendelet előírásai szerint szükség szerint képviselőt vagy kapcsolattartót jelöljön ki, aki az adatkezeléssel összefüggő ügyekben (pl. incidens bejelentése, stb.) kapcsolattartó pontként szolgál az érintettekkel, felügyeleti hatósággal (NAIH), valamint adott esetben bármely egyéb kérdésben konzultációt folytathat vele. Megvizsgálja, köteles-e Adatvédelmi tisztviselőt kinevezni, vagy önként sor kerül-e kinevezésére. Felelőssége a kapcsolattartóval kapcsolatos bármilyen módosulást, változást azonnal, késedelem nélkül az érintettek tudomására hozni (tájékoztató, bejelentés, stb.).

1.10. Adatvédelmi tisztviselő

A vezető nevezi ki az Adatvédelmi tisztviselőt, akinek kinevezését, jogállását lásd a *2.1. Adatvédelmi tisztviselő kijelölése* fejezetnél.

1.11. Képzés

A vezető jóváhagyta a szükséges felkészültséget, kompetenciát valamennyi munkatársa, illetve a vele szerződéses jogviszonyban álló valamennyi magánszemély és szervezet/intézmény esetében, amelynek munkavállalói vagy alvállalkozói a szervezet által használt rendszerekhez, személyes adatokhoz, adatkezelési műveletekhez hozzáféréssel rendelkeznek, illetve akik részt vesznek a szervezetnél keletkezett, feldolgozott, tárolt, illetve továbbított személyes adatok kezelésében. Feladata, hogy biztosítsa az adatkezelési műveletekben résztvevő külső és belső munkatársak folyamatos tudatosság-növelését, hogy felkészültek legyenek a megfelelő oktatások, képzések, gyakorlat alapján.

Felelőssége, hogy folyamatosan kiértékelje az elvégzett tevékenységek eredményességét, biztosítsa, hogy a munkatársak tudatában legyenek az adatkezelési/adatfeldolgozási tevékenységében betöltött szerepüknek és annak fontosságának.

Feladata, hogy felmérje a képzési szükségleteket és megszervezze az adatkezeléssel kapcsolatos külső és belső oktatásokat, képzéseket, és ezekről a megfelelő feljegyzéseket (pl. Oktatási tematika, Oktatási napló, stb.) megőrizze. Szükség szerinti gyakorisággal, legalább évente egyszer képzést szervez vagy online képzést tart, ahol ismertetésre kerül a Rendeletet és jelen Adatvédelmi és adatbiztonsági szabályzat előírásai. Cél a munkatársak és a közreműködők tudatosság-növelése és folyamatos továbbképzése, a szervezeti adatvédelmi szabályok fontosságának előtérbe helyezése, bemutatása.

Felelőssége a személyes adatokba állandó jelleggel vagy rendszeresen betekintő személyzetnek nyújtandó megfelelő személyre szóló adatvédelmi továbbképzés szervezése, valamint közös képzési és csereprogramok (pl. felügyeleti hatóságok között, valamint adott esetben harmadik országok felügyeleti hatóságaival vagy nemzetközi szervezetekkel) támogatása.

2. A szervezet adatvédelmi feladatai

2.1. Adatvédelmi tisztviselő kijelölése

Kötelező a kinevezés, mivel az adatkezelést közhatalmi szerv vagy egyéb, közfeladatot ellátó szerv végzi.

Az Adatvédelmi tisztviselőt a szakmai rátermettsége és különösen az adatvédelmi jog és gyakorlat szakértői szintű ismerete, valamint a Rendeletben az Adatvédelmi tisztviselő feladatai között felsorolt feladatok ellátására való alkalmassága alapján kell megbízni.

Közhatalmi szerv vagy egyéb, közfeladatot ellátó szerv közös Adatvédelmi tisztviselőt jelölhet ki több ilyen szerv számára, az adott szervek szervezeti felépítésének és méretének figyelembevételével.

A Szervezet támogatása az Adatvédelmi tisztviselő munkájához:

- biztosítja, hogy az Adatvédelmi tisztviselő a személyes adatok védelmével kapcsolatos összes ügybe megfelelő módon és időben bekapcsolódjon,
- biztosítja azokat a forrásokat, amelyek e feladatok végrehajtásához, a személyes adatokhoz és az adatkezelési műveletekhez való hozzáféréshez, valamint az Adatvédelmi tisztviselő szakértői szintű ismereteinek fenntartásához szükségesek,
- biztosítja, hogy az Adatvédelmi tisztviselő a feladatai ellátásával kapcsolatban utasításokat senkitől ne fogadjon el, őt a feladatai ellátásával összefüggésben nem bocsáthatja el, és szankcióval nem sújthatja,
- az Adatvédelmi tisztviselőt minden személyes adattal kapcsolatos, személyes adatot érintő kérdésbe bevonja,
- önállóan vagy közös Adatvédelmi tisztviselő által képviselt szervezetekre vonatkozóan együttesen biztosít az Adatvédelmi tisztviselő hatósági bejelentése, kommunikációja és az érintettekkel való közvetlen és folyamatos kapcsolattartás érdekében egy – lehetőleg kizárólag erre a célra szolgáló – e-mail-címet, ehhez a tisztviselő számára hozzáférést (pl. adatvedelem@domain.hu).

Az Adatvédelmi tisztviselő jogállása:

- az Adatvédelmi tisztviselő közvetlenül a Szervezet vezetőjének tartozik felelősséggel,
- az érintettek a személyes adataik kezeléséhez és a Rendelet szerinti jogaik gyakorlásához kapcsolódó valamennyi kérdésben az Adatvédelmi tisztviselőhöz fordulhatnak,
- feladatai teljesítésével kapcsolatban uniós vagy tagállami jogban meghatározott titoktartási kötelezettség vagy az adatok bizalmas kezelésére vonatkozó kötelezettség köti,
- az Adatvédelmi tisztviselő más feladatokat is elláthat, a vezetés biztosítja, hogy e feladatokból ne fakadjon összeférhetetlenség.

Az Adatvédelmi tisztviselő legalább a következő feladatokat látja el:

- tájékoztat és szakmai tanácsot ad a vezetőség, továbbá az adatkezelést végző alkalmazottak, közreműködők részére a Rendelet, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezések szerinti kötelezettségeikkel kapcsolatban,

- ellenőrzi a Rendeletnek, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezéseknek, továbbá a Szervezet 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,
- kérésre szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, valamint nyomon követi a hatásvizsgálat elvégzését,
- együttműködik a felügyeleti hatósággal,
- az adatkezeléssel összefüggő ügyekben – ideértve az előzetes konzultációt is – kapcsolattartó pontként szolgál a felügyeleti hatóság felé, valamint adott esetben bármely egyéb kérdésben konzultációt folytat vele.

Az Adatvédelmi tisztviselő jogviszonyának fennállása alatt és azt követően is köteles titokként megőrizni a vonatkozó tevékenységével kapcsolatban tudomására jutott azon személyes adatot, minősített adatot, törvény által titoknak minősített adatot, illetve minden olyan adatot, tényt vagy körülményt, amelyet az őt alkalmazó adatkezelő vagy adatfeldolgozó törvény előírása alapján nem köteles nyilvánosságra hozni.

A Rendelet 37. cikk (7) bekezdése szerint az adatkezelőnek vagy adatfeldolgozónak az általa kijelölt Adatvédelmi tisztviselő elérhetőségét közzé kell tennie és erről tájékoztatnia kell az illetékes felügyeleti hatóságot. Az Infotv. 25/L. § (4) bekezdése szerint az adatkezelő, illetve az adatfeldolgozó tájékoztatja a Hatóságot az Adatvédelmi tisztviselő nevééről, postai és elektronikus levélcíméről, ezen adatok változásáról, valamint ezen adatokat nyilvánosságra hozza. A Nemzeti Adatvédelmi és Információszabadság Hatóság az adatkezelők, illetve adatfeldolgozók számára külön erre a célra létrehozott elektronikus felületen is lehetővé teszi az Adatvédelmi tisztviselő bejelentését.

A Szikszói Közös Önkormányzati Hivatal az Adatvédelmi tisztviselő kijelölést, azzal kapcsolatos információkat (pl. jogállás), a tisztviselő adatait a GDPR Reg Adatkezelési rendszerben dokumentálja, tartja nyilván.

Az aktuálisan szereplő adatok feltüntetésre kerülnek az adatkezelési tájékoztatókban és valamennyi dokumentumban.

2.2. Adatkezelési, adatfeldolgozói tevékenységek nyilvántartása

A Szikszói Közös Önkormányzati Hivatal egyes adatkezelések tekintetében:

- önálló adatkezelőnek minősül (a személyes adatok kezelésének céljait és eszközeit önállóan határozza meg)
- közös adatkezelőnek minősülhet (a személyes adatok kezelésének céljait és eszközeit másokkal együtt határozza meg)
- adatfeldolgozónak minősülhet (valamely adatkezelő nevében személyes adatokat kezel)

A Szervezet, mint adatkezelő és adatfeldolgozó a felelősségébe tartozóan végzett adatkezelési, adatfeldolgozói tevékenységekről nyilvántartást vezet, mivel a Rendelet alapján nem mentesül a nyilvántartás-vezetési kötelezettség alól, valamint így tudja teljesíteni az elszámoltathatóság elvét, mely szerint az adatkezelő felelős a személyes adatok kezelésére vonatkozó elveknek (lásd 1.4 fejezet) való megfelelésért, továbbá képesnek kell lennie e megfelelés igazolására. A nyilvántartásokat a felügyeleti hatóság részére rendelkezésre bocsátja.

Az Adatkezelési nyilvántartás a következő információkat tartalmazza:

- az adatkezelő neve és elérhetősége, valamint – ha van ilyen – a közös adatkezelőnek, az adatkezelő képviselőjének és az Adatvédelmi tisztviselőnek a neve és elérhetősége;
- az adatkezelés céljai;
- az érintettek kategóriáinak, valamint a személyes adatok kategóriáinak ismertetése;
- olyan címzettek kategóriái, akikkel a személyes adatokat közlik vagy közölni fogják, ideértve a harmadik országbeli címzetteket vagy nemzetközi szervezeteket;
- 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 továbbítás esetében a megfelelő garanciák leírása;
- ha lehetséges, a különböző adatkategóriák törlésére előírányzott határidők;
- ha lehetséges, a technikai és szervezési intézkedések általános leírása.

Ha van olyan adatkezelés, ahol a Szervezet adatfeldolgozónak minősül, akkor szükséges az adatfeldolgozói nyilvántartás, mely a következő információkat tartalmazza:

- 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;
- az egyes adatkezelők nevében végzett adatkezelési tevékenységek kategóriái;
- adott esetben a személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítása, beleértve a harmadik ország vagy a nemzetközi szervezet azonosítását, valamint továbbítás esetében a megfelelő garanciák leírása;
- ha lehetséges, a technikai és szervezési intézkedések általános leírása.

A Szikszói Közös Önkormányzati Hivatal az adatkezelési, adatfeldolgozói tevékenységeket a GDPR Reg Adatkezelési rendszerben tartja nyilván. Az adatkezelő és az adatfeldolgozó nevében végzett adatkezelési tevékenységek nyilvántartásai a Rendelet követelményei szerinti, aktuális adattartalommal tartalmazza rendszerben szereplő, egyedileg rögzített adatkezeléseket.

2.3. Átlátható tájékoztatás, kommunikáció és az érintett jogainak gyakorlására vonatkozó intézkedések

A Szervezet megfelelő intézkedéseket hozott annak érdekében, hogy az érintett (bármely információ alapján azonosított vagy azonosítható természetes személy) részére a személyes adatok kezelésére vonatkozó valamennyi tájékoztatást tömör, átlátható, érthető és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazva nyújtsa, különösen a gyermekeknek címzett bármely információ esetében. Az információkat írásban vagy más módon – ideértve adott esetben az elektronikus utat is – kell megadni. Az érintett kérésére szóbeli tájékoztatás is adható, feltéve, hogy más módon igazolásra kerül az érintett személyazonossága. Az érintetti kérelmek kezelését lásd a 2.4 fejezetben.

2.3.1. Tájékoztatás és a személyes adatokhoz való hozzáférés joga

Ha az érintettre vonatkozó személyes adatokat az érintettől gyűjtik, akkor az átlátható tájékoztatás és a személyes adatokhoz való hozzáférés joga érdekében az adatkezelő az adatok megszerzésének időpontjában, illetve az adatkezelés megkezdését megelőzően Adatkezelési tájékoztatókban vagy egyéb módon az érintettek rendelkezésére bocsátja a Rendeletben előírt információkat:

- a munkáltatói szerepkörben, a munkaviszonyhoz vagy egyéb foglalkoztatásra irányuló jogviszonyhoz kapcsolódóan folytatott adatkezelési műveletekre vonatkozó adatkezelésekről írásban tájékoztatja a munkavállalókat, a tudomásulvétel feljegyzését megőrzi;
- a tevékenységével kapcsolatos adatkezelésekről (pl. hatósági eljárások során végzett adatkezelésekről) az ügyfeleket egy vagy több adatkezelési tájékoztatóban tájékoztatja, a tájékoztató minden olyan helyen rendelkezésre áll elektronikus vagy nyomtatott formában, ahol szükséges az érintettek tájékoztatása;
- további adatkezelések, főként az információs társadalommal összefüggő szolgáltatások (elektronikus úton, távollevők részére nyújtott szolgáltatás) esetén az adatkezelési tájékoztatót az érintettek előzetes tájékoztatására elektronikusan, internetes honlapon, digitális formában, bárki számára, személyazonosítás nélkül, korlátozástól mentesen hozzáférhetővé teszi. A közfeladatot ellátó szervek az elektronikus közzétételt saját vagy társulásai által közösen működtetett, illetve a felügyeletüket, szakmai irányításukat vagy működésükkel kapcsolatos koordinációt ellátó szervek által fenntartott, erre a célra létrehozott központi honlapon való közzététellel biztosíthatják;
- ha a személyes adatokon a gyűjtésük céljától eltérő célból további adatkezelést kíván végezni, a további adatkezelést megelőzően tájékoztatja az érintettet erről az eltérő célról és minden releváns kiegészítő információról;
- az érintett rendelkezésére bocsátandó információkra vonatkozó szabályok nem alkalmazandóak, ha és amilyen mértékben az érintett már rendelkezik az információkkal.

Az Adatkezelési tájékoztató tartalmazza az alábbiakat:

- az adatkezelőnek és – ha van ilyen – az adatkezelő képviselőjének a kiléte és elérhetőségei,
- az Adatvédelmi tisztviselő elérhetőségei,
- a személyes adatok tervezett kezelésének célja,
- az adatkezelés jogalapja,
- a személyes adat szolgáltatása jogszabályon vagy szerződéses kötelezettségen alapul vagy szerződés kötésének előfeltétele-e, valamint hogy az érintett köteles-e a személyes adatokat megadni, továbbá hogy milyen lehetséges következményekkel járhat az adatszolgáltatás elmaradása,
- ha az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, akkor az adatkezelő, vagy harmadik fél jogos érdekei,
- a személyes adatok tárolásának időtartama, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjai,
- adott esetben a személyes adatok címzettjei, illetve a címzettek kategóriái, ha van ilyen,
- adott esetben annak ténye, hogy az adatkezelő harmadik országba vagy nemzetközi szervezet részére kívánja továbbítani a személyes adatokat,
- automatizált döntéshozatal ténye, ideértve a profilalkotást is, valamint legalább ezekben az esetekben az alkalmazott logikára és arra vonatkozóan érthető információk, hogy az ilyen adatkezelés milyen jelentőséggel, és az érintettre nézve milyen várható következményekkel bír,

- tájékoztatás az érintett azon jogáról, hogy kérelmezheti az adatkezelőtől a rá vonatkozó személyes adatokhoz való hozzáférést, azok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen, valamint az érintett adathordozhatósághoz való joga,
- az érintett hozzájárulásán alapuló adatkezelés esetén a hozzájárulás bármely időpontban történő visszavonásához való jog, amely nem érinti a visszavonás előtt a hozzájárulás alapján végrehajtott adatkezelés jogszerűségét,
- a felügyeleti hatósághoz címzett panasz benyújtásának joga.

Ha az érintettre vonatkozó személyes adatokat nem az érintettől gyűjtik: az adatkezelőnek az adatkezelési tájékoztatás során fentiekén kívül rendelkezésre bocsátani a személyes adatok forrását és adott esetben azt, hogy az adatok nyilvánosan hozzáférhető forrásokból származnak-e.

A tájékoztatást a személyes adatok kezelésének konkrét körülményeit tekintetbe véve, a személyes adatok megszerzésétől számított észszerű határidőn, de legkésőbb egy hónapon belül, ha a személyes adatokat az érintettel való kapcsolattartás céljára használják, legalább az érintettel való első kapcsolatfelvétel alkalmával, vagy ha várhatóan más címmel is közlik az adatokat, legkésőbb a személyes adatok első alkalommal való közlésekor kell megadni.

Az érintett rendelkezésére bocsátandó információkra vonatkozó szabályok nem alkalmazandóak, ha és amilyen mértékben az érintett már rendelkezik az információkkal, az információk rendelkezésre bocsátása lehetetlennek bizonyul vagy aránytalanul nagy erőfeszítést igényelne, az adat megszerzését vagy közlését kifejezetten előírja az adatkezelőre alkalmazandó uniós vagy tagállami jog, vagy a személyes adatoknak valamely uniós vagy tagállami jogban előírt szakmai titoktartási kötelezettség alapján bizalmasnak kell maradnia.

A Szikszói Közös Önkormányzati Hivatal az érintettek tájékoztatóit a Rendelet követelményei szerinti adattartalommal GDPR Reg Adatkezelési rendszerben készíti el az előzetesen egyedileg összeállított, folyamatosan aktualizált adatkezelések adataival.

A szerkeszthető adatkezelési tájékoztatók kategóriánként generálhatók, abból a célból, hogy személyre szabott tájékoztatóval tudja tájékoztatni az érintetteket (készülnek munkavállalói, ügyfelekkel kapcsolatos, és szakmai, valamint egyedileg létrehozott kategóriával kapcsolatos adatkezelési tájékoztatók, ha vannak).

Az Ügyfelekkel kapcsolatos aktuális adatkezelési tájékoztató honlapon is publikálásra kerül, ennek megkönnyítésére lehetséges a tájékoztatót tartalmazó weboldal domain nevéhez egyedi un. API kód generálása. A weboldalt üzemeltető által elvégzett egyszeri kódbeillesztést követően automatikusan megjelenik a weboldalon az ügyfelekkel kapcsolatos aktuális adatkezelési tájékoztató.

2.3.2. Az érintett hozzáférési joga

Az adatkezelés teljes tartama alatt az érintett jogosult a megadott elérhetőségeken tájékoztatást és hozzáférést kérni az adatkezelő által kezelt személyes adatokról, valamint az adatkezelés jellemzőiről:

- az adatkezelés céljáról,
- az érintett személyes adatok kategóriáiról,
- a címzettekről vagy címzettek kategóriáiról, akikkel, illetve amelyekkel a személyes adatokat közltek vagy közölni fogják, különösen a harmadik országbeli címzetteket, nemzetközi szervezeteket,

- a személyes adatok tárolásának tervezett időtartamáról, vagy az időtartam meghatározásának szempontjairól,
- az érintett személyes adatai kezelésével kapcsolatos helyesbítési, törlési, korlátozási vagy tiltakozási jogairól,
- a valamely felügyeleti hatósághoz címzett panasz benyújtásának jogáról,
- ha az adatokat nem az érintettől gyűjtötték, a forrásukra vonatkozó minden elérhető információról,
- az automatizált döntéshozatal tényéről, ideértve a profilalkotást is, az alkalmazott logikára és arra vonatkozó érthető információkról, hogy az ilyen adatkezelés milyen jelentőséggel bír, és az érintettre nézve milyen várható következményekkel jár,
- a valamely felügyeleti hatósághoz címzett panasz benyújtásának jogáról,
- illetve a Tájékoztatás és a személyes adatokhoz való hozzáférés joga alapján a 2.3.1 pontban felsorolt valamennyi információról (ami az adatkezelési tájékoztató kötelező tartalmi eleme).

A személyes adatoknak harmadik országba vagy nemzetközi szervezet részére történő továbbítása esetén az érintett jogosult arra, hogy tájékoztatást kapjon a továbbításra vonatkozóan az adattovábbítás megfelelő garanciáiról.

Az adatkezelő az érintett kérésére az adatkezelés tárgyát képező személyes adatok másolatát rendelkezésére bocsátja. Lásd a 2.4. *Érintetti kérelmek kezelése* fejezetet.

2.3.3. Az érintett helyesbítéshez való joga

Az érintett jogosult kérelmezni személyes adatainak helyesbítését. Amennyiben adatai megváltoztak, vagy nem pontosak, akkor kérelmére - a személyes adatok kezelésének ideje alatt - bármikor módosítja azokat az adatkezelő.

2.3.4. A törléshez, elfeledtetéshez való jog

Az Érintett hozzájárulásán alapuló adatkezelés esetén az érintett bármikor visszavonhatja hozzájárulását és kérheti, hogy adatait törölje az adatkezelő, amennyiben az adatkezelésnek nincs további jogalapja. A visszavonás nem érinti a visszavonás előtt a hozzájárulás alapján végrehajtott adatkezelés jogszerűségét.

Az érintett az alábbi indokok valamelyikének fennállása esetén jogosult arra, hogy kérésére az adatkezelő indokolatlan késedelem nélkül törölje a rá vonatkozó személyes adatokat:

- személyes adatokra már nincs szükség abból a célból, amelyből azokat gyűjtötték vagy más módon kezelték;
- az érintett visszavonja az adatkezelés alapját képező hozzájárulását, és az adatkezelésnek nincs más jogalapja;
- az érintett tiltakozik az adatkezelés ellen, és nincs elsőbbséget élvező jogszerű ok az adatkezelésre;
- a személyes adatokat jogellenesen kezelték;
- a személyes adatokat az adatkezelőre alkalmazandó uniós vagy tagállami jogban előírt jogi kötelezettség teljesítéséhez törölni kell;
- a személyes adatok gyűjtésére információs társadalommal összefüggő szolgáltatások kínálásával kapcsolatosan került sor.

Az adatok törlési kérelme elutasítható, ha az adatkezelés szükséges:

- a véleménynyilvánítás szabadságához és a tájékozódáshoz való jog gyakorlása céljából;

- 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;
- közérdekből vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlása keretében végzett feladat végrehajtása céljából;
- a népegészségügy területét érintő közérdekből;
- a közérdekű archiválás, tudományos és történelmi kutatási vagy statisztikai célból, ha a törlési jog valószínűsíthetően lehetetlenné tenné vagy komolyan veszélyeztetné ezt az adatkezelést.

Ha az adatkezelő nyilvánosságra hozta a személyes adatot, és azt törölni köteles, az elérhető technológia és a megvalósítás költségeinek figyelembevételével megteszi az észszerűen elvárható lépéseket – ideértve technikai intézkedéseket – annak érdekében, hogy tájékoztassa az adatokat kezelő adatkezelőket, hogy az érintett kérelmezte tőlük a szóban forgó személyes adatokra mutató linkek vagy e személyes adatok másolatának, illetve másodpéldányának törlését.

2.3.5. Az adatkezelés korlátozásához való jog

Az adatkezelő korlátozza a személyes adatok kezelését, ha ezt kéri az érintett. Az érintett a következő esetekben kérheti az adatai korlátozását:

- amennyiben vitatja adatai pontosságát, ez esetben a korlátozás arra az időtartamra vonatkozik, amely lehetővé teszi, hogy az adatkezelő ellenőrizze a személyes adatok pontosságát;
- amennyiben az adatkezelés jogellenes és az érintett ellenzi adatainak törlését és ehelyett kéri azok korlátozását;
- az adatkezelőnek már nincs szüksége a személyes adatokra az adatkezelés céljából, de az érintett igényli azokat jogi igényének előterjesztéséhez, érvényesítéséhez vagy védelméhez;
- az érintett tiltakozik az adatkezelés ellen, ez esetben a korlátozás arra az időtartamra vonatkozik, amíg megállapításra nem kerül, hogy az adatkezelő jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben.

Ha az adatkezelés korlátozás alá esik, a személyes adatokat a tárolás kivételével csak az érintett hozzájárulásával, valamint jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez, vagy más természetes vagy jogi személy jogainak védelme érdekében, vagy az Unió, illetve valamely tagállam fontos közérdekből lehet kezelni. Az érintettet az adatkezelés korlátozásának feloldásáról előzetesen tájékoztatni kell.

A személyes adatok kezelésének korlátozására alkalmazott módszerek közé tartozhat többek között a szóban forgó személyes adatoknak egy másik adatkezelő rendszerbe történő ideiglenes áthelyezése vagy a felhasználók számára való hozzáférhetőségük megszüntetése, illetve egy honlapról az ott közzétett adatok ideiglenes eltávolítása. Az adatkezelés korlátozását az automatizált nyilvántartási rendszerekben alapvetően technikai eszközökkel kell biztosítani, oly módon, hogy a személyes adatokon további adatkezelési műveleteket ne végezzenek el és azokat ne lehessen megváltoztatni. Azt a tényt, hogy a személyes adatok kezelése korlátozott, egyértelműen jelezni kell a rendszerben.

2.3.6. A személyes adatok helyesbítéséhez vagy törléséhez, illetve az adatkezelés korlátozásához kapcsolódó értesítési kötelezettség

Minden olyan címzettet tájékoztatni kell a helyesbítésről, törlésről vagy adatkezelés-korlátozásról, akivel, illetve amellyel a személyes adat közlésre került, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel. Az érintettet kérésére az adatkezelő tájékoztatja e címzettekről.

2.3.7. Az adathordozhatósághoz való jog

Ha az adatkezelés hozzájáruláson alapul, vagy szerződés teljesítéséhez szükséges és az adatkezelés automatizált módon történik, az érintettek adatait gépi nyilvántartással kezelik, az érintett jogosult arra, hogy a rá vonatkozó, az általa az adatkezelő rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja, ezeket egy másik adatkezelőnek továbbítsa. Jogosult arra, hogy – ha ez technikailag megvalósítható – kérje a személyes adatok adatkezelők közötti közvetlen továbbítását. Az adatok hordozhatóságához való jog nem érintheti hátrányosan mások jogait és szabadságait, illetve nem alkalmazandó abban az esetben, ha az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítványai gyakorlásának keretében végzett feladat végrehajtásához szükséges.

2.3.8. A tiltakozáshoz való jog

Az érintett jogosult saját helyzetével kapcsolatos okból bármikor tiltakozni személyes adatai kezelése ellen, ha adatkezelő az adatokat saját vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges vagy közérdekű/adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges jogalapról kezeli, ideértve az említett rendelkezéseken alapuló profilalkotást is. A tiltakozási jogára legkésőbb az érintettel való első kapcsolatfelvétel során kifejezetten fel kell hívni a figyelmét, és az erre vonatkozó tájékoztatást egyértelműen, minden más információtól elkülönítve kell megjeleníteni. A tiltakozáshoz való jogot az információs társadalommal összefüggő szolgáltatások igénybevételéhez kapcsolódóan műszaki előírásokon alapuló automatizált eszközökkel is gyakorolhatja.

Tiltakozás esetén a személyes adatot nem kezelheti tovább az adatkezelő, kivéve, ha bizonyítja, hogy az adatkezelést olyan kényszerítő erejű jogos okok indokolják, amelyek elsőbbséget élveznek az érintett érdekeivel, jogaival és szabadságával szemben, vagy amelyek jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódnak. Tudományos és történelmi kutatási vagy statisztikai célú adatkezelés esetén az érintett nem élhet tiltakozási jogával, ha az adatkezelésre közérdekű okból végzett feladat végrehajtása érdekében van szükség.

Tiltakozás közvetlen üzletszerzés esetén: Az érintett tiltakozhat, ha a személyes adatok kezelése közvetlen üzletszerzés érdekében történik, ideértve a profilalkotást is, amennyiben az a közvetlen üzletszerzéshez kapcsolódik. Ha tiltakozik a személyes adatok közvetlen üzletszerzés érdekében történő kezelése ellen, akkor a személyes adatok a továbbiakban e célból nem kezelhetők.

2.3.9. Automatizált döntéshozatal egyedi ügyekben, profilalkotás

Az érintett jogosult arra, hogy ne terjedjen ki rá az olyan, kizárólag automatizált adatkezelésen – ideértve a profilalkotást is – alapuló döntés hatálya, amely rá nézve joghatással járna vagy őt hasonlóképpen jelentős mértékben érintené.

Nem alkalmazható a fenti jogosultság, ha az automatizált döntéshozatal:

- az érintett és az adatkezelő közötti szerződés megkötése vagy teljesítése érdekében szükséges,

- meghozatalát az adatkezelőre alkalmazandó olyan uniós vagy tagállami jog teszi lehetővé, amely az érintett jogainak és szabadságainak, valamint jogos érdekeinek védelmét szolgáló megfelelő intézkedéseket is megállapít,
- az érintett kifejezett hozzájárulásán alapul.

A szerződés megkötése vagy teljesítése érdekében szükséges vagy az érintett kifejezett hozzájárulásán alapuló adatkezelések esetén megfelelő intézkedéseket kell tenni az érintett jogainak, szabadságainak és jogos érdekeinek védelme érdekében, ideértve az érintettnek legalább azt a jogát, hogy az adatkezelő részéről emberi beavatkozást kérjen, álláspontját kifejezze, és a döntéssel szemben kifogást nyújtson be.

Az automatizált döntéshozatal nem alapulhat a személyes adatoknak különleges kategóriáin, kivéve ha az érintett kifejezett hozzájárulását adta vagy az adatkezelés jelentős közérdek miatt szükséges, uniós jog vagy tagállami jog alapján, és az érintett jogainak, szabadságainak és jogos érdekeinek védelme érdekében megfelelő intézkedések megtételére került sor.

2.3.10. A személyes adatokkal összefüggő jogok érvényesítése az érintett halálát követően

Az Infotv. szerint az érintett halálát követő öt éven belül a Rendelet hatálya alá tartozó adatkezelési műveletek esetén az elhatalt életében megillető egyes jogokat (a hozzáféréshez és a törléshez való jogokat) az érintett által arra ügyintézési rendelkezéssel, illetve közokiratban vagy teljes bizonyító erejű magánokiratban foglalt, az adatkezelőnél tett nyilatkozattal - ha az érintett egy adatkezelőnél több nyilatkozatot tett, a későbbi időpontban tett nyilatkozattal - meghatalmazott személy jogosult érvényesíteni.

Ha az érintett nem tett megfelelő jognyilatkozatot, a Ptk. szerinti közeli hozzátartozója annak hiányában is jogosult a Rendelet hatálya alá tartozó adatkezelési műveletek esetén a helyesbítéshez és tiltakozáshoz való jogot, valamint - ha az adatkezelés már az érintett életében is jogellenes volt vagy az adatkezelés célja az érintett halálával megszűnt – a Rendelet hatálya alá tartozó adatkezelési műveletek esetén a Rendeletben az adatkezelés korlátozásához, törléshez való jogot, mint az elhatalt életében megillető jogokat érvényesíteni az érintett halálát követő öt éven belül. Az érintett jogainak e bekezdés szerinti érvényesítésére az a közeli hozzátartozó jogosult, aki ezen jogosultságát elsőként gyakorolja.

Az érintett jogait érvényesítő személyt e jogok érvényesítése - így különösen az adatkezelővel szembeni, valamint a Hatóság, illetve bíróság előtti eljárás - során az e törvény által az érintett részére megállapított jogok illetik meg és kötelezettségek terhelik.

Kérelemre tájékoztatni kell az érintett Ptk. szerinti közeli hozzátartozóját megtett intézkedésekről, kivéve, ha azt az érintett nyilatkozatában megtiltotta.

2.4. Az érintetti kérelmek kezelése

Az érintett magánszemélynek, személy azonosítása mellett lehetősége van bármely általa választott módon kérelmet benyújtani személyesen, postai úton, elektronikus levélben, meghatalmazott útján, illetve egyéb módon. A tájékoztatást az érintett által kért módon kell megadni, elektronikus úton benyújtott kérelem esetén lehetőség szerint elektronikus úton kell megadni.

A Szikszói Közös Önkormányzati Hivatal megfelelő intézkedéseket hozott annak érdekében, hogy az érintett részére a személyes adatok kezelésére vonatkozó valamennyi tájékoztatást tömör, átlátható, érthető és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazva nyújtsa. Az információkat írásban vagy más módon – ideértve adott esetben az elektronikus utat is – kell megadni. Az érintett kérésére szóbeli tájékoztatás is adható, feltéve, hogy más módon igazolásra kerül az érintett személyazonossága.

Indokolatlan késedelem nélkül, de legfeljebb a kérelem beérkezésétől számított egy hónapon belül tájékoztatja az érintettet jogai gyakorlására irányuló kérelmében foglaltak teljesítéséről, a kérelem nyomán hozott intézkedésekről. Szükség esetén, figyelembe véve a kérelem összetettségét és a kérelmek számát, ez a határidő további két hónappal meghosszabbítható.

Ha nem tesz intézkedéseket az érintett kérelme nyomán, késedelem nélkül, de legkésőbb a kérelem beérkezésétől számított egy hónapon belül tájékoztatja az érintettet az intézkedés elmaradásának okairól, a késedelem okainak megjelölésével, valamint arról, hogy az érintett panaszt nyújthat be valamely felügyeleti hatóságnál, és élhet bírósági jogorvoslati jogával.

Amennyiben úgy ítéli meg, hogy az érintett magánszemély kérelmének teljesítésére nincs lehetőség, úgy a kérelem elutasításáról és a Rendelet szerinti jogorvoslati jogokról tájékoztatja a kérelmezőt.

Az érintetti kérelmek kezelése, teljesítése a Szervezet vezetője vagy az általa kijelölt személy feladata. Indokolt esetben be kell vonni az Adatvédelmi tisztviselőt vagy jogi szakértőt.

A Szervezet biztosítja a jogot az érintettek számára, hogy a felügyeleti hatósághoz történő panasztétellel párhuzamosan bírósági jogorvoslatot is igényeljenek, amennyiben megítélésük szerint valamely adatkezelő vagy adatfeldolgozó a személyes adataiknak kezelése során megsértette adatvédelemre vonatkozó jogait. Az érintett által kezdeményezett bírósági eljárás során nem az érintettnek kell bizonyítania adatvédelemmel kapcsolatos jogai megsértését, hanem az adatkezelő vagy adatfeldolgozó köteles bizonyítani azt, hogy az érintett ezen jogai nem sérültek.

Adatkezelő a kérelem benyújtásakor jogosult és köteles ellenőrizni a kérelmező személyazonosságát az adatok bizalmassága és jogi kötelezettségek teljesítése érdekében. Az azonosítás lehetőség szerint az adatmegadás, adatszerzés módjához kapcsolódik. Érintetti kérelem alapján történő eljárás esetén az adatigénylő személyazonosító adatai csak annyiban kezelhetők, amennyiben az az igény teljesítéséhez - beleértve az esetleges költségek megfizetését is - elengedhetetlenül szükséges.

A Szervezet az érintetti tájékoztatások, kérelmek elbírálása és teljesítése során tevékenységéért költséget, díjazást nem számol fel, de az egyértelműen megalapozatlan vagy ismételt, túlzó jellegű kérelmek esetén, figyelemmel a kért információ vagy tájékoztatás nyújtásával vagy a kért intézkedés meghozatalával járó adminisztratív költségekre, jogosult észszerű összegű díj felszámítására, illetve megtagadhatja a kérelem alapján történő intézkedést. A kérelem egyértelműen megalapozatlan vagy túlzó jellegének bizonyítása az adatkezelőt terheli. Erre vonatkozó rendelkezéshiányában a kérelem teljesítéséért megállapítható költségek a 301/2016. (IX. 30.) Korm. rendeletben foglalt költségek figyelembevételével kerülnek megállításra.

A Szikszói Közös Önkormányzati Hivatal az érintettek kérelmeit a GDPR Reg Adatkezelési rendszerben is nyilvántarthatja, elkészítheti a szükséges dokumentumokat. A rendszer támogatja az adatkezelőt az érintett magánszemélyek GPRG Rendelet 15–22. cikk szerinti jogainak a gyakorlásával kapcsolatos feladatokban. A generált szerkeszthető dokumentum tartalmazza az adatkezelő és az érintett kérelmező főbb adatait, a kiválasztott adatkezelés(ek) leírását és tájékoztatást a panasz benyújtáshoz vagy bírósági jogorvoslati jogról.

2.5. Az adatkezelés biztonsága, technikai és szervezési intézkedések végrehajtása

A Szikszói Közös Önkormányzati Hivatal, mint adatkezelő és adatfeldolgozó a felelősségébe tartozóan végzett adatkezelési, adatfeldolgozási tevékenységekkel kapcsolatban a tudomány és technológia állása és a megvalósítás költségei, továbbá 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 érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja.

A Szervezet vezetője felelős azért, hogy figyelembe véve a szervezet méretét, a folyamatok bonyolultságát és kölcsönhatását, a személyzet kompetenciáját, valamint a vonatkozó törvényeket, előírásokat, elvárásokat, meghatározza informatikai- és adatbiztonsági követelményrendszerét és környezetét.

Az adatkezelés biztonsága érdekében meghatározott technikai, szervezési intézkedéseket a 4.fejezet tartalmazza részletesen.

A Szikszói Közös Önkormányzati Hivatal a GDPR Reg Adatkezelési rendszerben is rögzítheti az adatkezelésekkel kapcsolatos technikai, szervezési intézkedéseket, az aktuális adatokkal a nyilvántartások nyomtathatóak.

2.6. Az adatvédelmi incidensek

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.

A Szikszói Közös Önkormányzati Hivatal, mint adatkezelő kötelessége, hogy amint tudomására jut egy adatvédelmi incidens (pl. felmerül a gyanú, hogy Szervezet számítógépes biztonsági incidens áldozatává vált, vagy éppen ennek folyamata alatt van) azt indokolatlan késedelem nélkül kivizsgálja, és szükség esetén bejelentse (ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott) az illetékes felügyeleti hatóságnál (NAIH).

A Szervezet, mint adatkezelő/adatfeldolgozó felelőssége megbizonyosodni arról, hogy az összes megfelelő technológiai védelmi és szervezési intézkedés végrehajtásra került-e, egyrészt az adatvédelmi incidens haladéktalan megállapítása, másrészt a felügyeleti hatóságnak történő bejelentés és az érintett sürgős értesítése érdekében. Azt, hogy az értesítésre indokolatlan késedelem nélkül került-e sor, különösen az adatvédelmi incidens jellegére és súlyosságára, valamint annak az érintettre gyakorolt következményeire, illetve hátrányos hatásaira figyelemmel kell megállapítani.

Ha a Szervezet adatfeldolgozónak minősül egyes adatkezelések tekintetében, a Rendeletben foglalt kötelezettségének megfelelően az arról való tudomásulvételt követően indokolatlan késedelem nélkül bejelenti az adatkezelőnek.

2.6.1. Incidensek belső nyilvántartása

Amennyiben az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve, akkor a Szervezet saját nyilvántartásába veszi.

2.6.2. Incidens NAIH bejelentése

Az érintettre nézve valószínűsíthető kockázat esetén bejelenti az incidenst a NAIH erre a célra szolgáló elektronikus Adatvédelmi Incidensbejelentő Rendszer felületén, vagy ennek hiányában postai úton. Ha nem lehetséges az információkat egyidejűleg közölni, akkor azok indokolatlan késedelem nélkül részletekben is közölhetők. Ha a bejelentés 72 órán belül nem történt meg, akkor a bejelentésben meg kell jelölni a késedelem okát.

A bejelentést a NAIH által elvárt adattartalommal kell teljesíteni. A szervezeti adatokon, az Adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó kapcsolattartó nevén és elérhetőségén kívül tartalmaznia kell:

- az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát;
- az adatvédelmi incidensből eredő, valószínűsíthető következményeket;
- adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

2.6.3. Érintettek tájékoztatása az Incidensről

Adatkezelő feladata, hogy az érintettet indokolatlan késedelem nélkül tájékoztassa abban az esetben, ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár jogaira és szabadságaira nézve, annak érdekében, hogy megtehessek a szükséges óvintézkedéseket. Az érintett részére adott tájékoztatásban a szervezeti adatokon, az Adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó kapcsolattartó nevén és elérhetőségén kívül világosan és közérthetően ismertetni kell az adatvédelmi incidens jellegét, az incidensből eredő, valószínűsíthető következményeket, az incidens orvoslására tett vagy tervezett intézkedéseket, adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

Az érintettek tájékoztatása mellőzhető ha:

- adatkezelő megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre, melyeket az incidens által érintett adatok tekintetében alkalmaztak (pl. a titkosítás, amely a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné tesz az adatokat),
- 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,
- a tájékoztatás aránytalan erőfeszítést tenne szükségessé - ilyen esetekben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, vagy olyan hasonló intézkedést kell hozni, amely biztosítja az érintettek hasonlóan hatékony tájékoztatását.

2.6.4. Adatvédelmi incidensek kezelése

Minden vélt vagy valós adatvédelmi incidensről késedelem nélkül, a megadott kapcsolattartási csatornák valamelyikén értesíteni kell az Adatvédelmi tisztviselőt vagy hiányában a kapcsolattartásra kijelölt felelőst vagy a Szervezet vezetőjét.

Az adatvédelmi incidenst észlelő személy köteles a tapasztalt jelenséget minden rendelkezésére álló eszközzel dokumentálni, azokat haladéktalanul az Adatvédelmi tisztviselő vagy hiányában a kijelölt felelős vagy vezető rendelkezésére bocsátani (pl. feljegyzés, képernyőkép, fotó, hibüzenet, stb.).

Az adatvédelmi incidens jelentésére vonatkozó kötelezettség valamennyi munkaviszony vagy foglalkoztatásra irányuló jogviszony alapján foglalkoztatottra, közreműködő munkatársra, valamint szerződéses, vagy más módon kapcsolatba kerülő természetes vagy jogi személyekre, gazdasági társaságokra, intézményekre vonatkozik, a velük kötött megállapodás, vagy titoktartási nyilatkozatok szerint.

A Szervezet vezetője által kijelölt felelős teendői:

- a körülmények ismeretében felméri a kockázatokat és meghatározza a kategóriát (nincs/van/magas kockázat),

- szükség esetén eseti szakértői csoportot hoz létre az incidens körülményeinek kivizsgálására, akik segítik a munkáját,
- értesíti a szervezet vezetőjét,
- meghatározza az értesítendő körét,
- amennyiben az adatbiztonsági incidens IT biztonsági esemény is egyben, intézkedést tesz annak megszüntetésére, vagy az esemény jellegéből adódóan annak izolálására (az izolálást azonnal meg kell kezdeni, az érintett felek bevonásával), az lbtv. hatálya alá tartozó szervezetek esetén késedelem nélkül értesíteni kell az elektronikus információs rendszerek biztonságáért felelős személyt is,
- meghatározza az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát,
- felméri az adatvédelmi incidensből eredő, valószínűsíthető következményeket,
- meghatározza az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket,
- az adatvédelmi incidensről, valamint annak életútjáról jegyzőkönyvet/nyilvántartást készít,
- indokolatlan késedelem nélkül bejelenti az illetékes Nemzeti Adatvédelmi és Információszabadság Hatóságnak, kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve,
- indokolatlan késedelem nélkül tájékoztatja az érintetteket az adatvédelmi incidensről, ha az valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve,
- amennyiben nem volt lehetséges az adatvédelmi incidenssel kapcsolatos információkat egyidejűleg közölni illetékes hatósággal, akkor azokat további indokolatlan késedelem nélkül később részletekben közli a hatósággal,
- irányítja a károk helyreállítását és a jogszerű működés visszaállítását,
- lezárja az adatvédelmi incidens kezelésének folyamatát és a kapcsolódó dokumentumokat,
- ellenőrzi a Rendeletnek, valamint a Szervezet személyes adatok védelmével kapcsolatos belső szabályainak való megfelelést, valamint áttekinti az érintettek jogainak védelmét szolgáló korrekciós intézkedéseket biztosító mechanizmusokat, és az incidensek kezelésére vonatkozó intézkedéseket, és azok eredményességét. Az ellenőrzés tapasztalatai szükség szerint beépülhetnek az adatvédelmi szabályozásba, illetve részét képezhetik a munkatársak képzésének, tovább képzésének.

A Szikszói Közös Önkormányzati Hivatal az adatvédelmi incidensek nyilvántartására, a hatósági adatszolgáltatásra a GDPR Reg Adatkezelési rendszert alkalmazza, melyben a NAIH által elvárt minimális adattartalommal rögzíthetők az incidensekkel kapcsolatos adatok, azokból a hatóság számára benyújtható dokumentum generálható.

2.7. Érdekmérlegelés

Az adatkezelő – ideértve azt az adatkezelőt is, akivel a személyes adatokat közölhetik – vagy valamely harmadik fél jogos érdeke jogalapot teremthet az adatkezelésre, feltéve hogy az érintett érdekei, alapvető jogai és szabadságai nem élveznek elsőbbséget, figyelembe véve az adatkezelővel való kapcsolata alapján az érintett észszerű elvárásait. Jogos érdekről lehet szó, amikor releváns és megfelelő kapcsolat áll fenn az érintett és az adatkezelő között, például olyan esetekben, amikor az érintett az adatkezelő ügyfele vagy annak alkalmazásában áll, vagy személyes adatok közvetlen üzletszerzési célú kezelése esetén.

Közhatalmi szervek esetén a jogalkotó feladata, hogy jogszabályban határozza meg, a kötelező adatkezelések részleteit. A jogos érdekre hivatkozást, mint jogalapot nem lehet alkalmazni a közhatalmi szervek által feladataik ellátása során végzett adatkezelésre.

Az adatkezelés akkor lehet jogszerű az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges jogalapra hivatkozással, ha adatkezelő a jogos érdek fennállásának megállapításához elvégezte az érdekmérlegelési tesztet, annak eredménye az, hogy az adatkezelés szükséges és arányos, adatkezelő jogos érdeke megállapítható.

Az érdekmérlegelés során megállapításra kerül, hogy az érintett magánszemély személyhez fűződő jogait az adatkezelés milyen mértékben korlátozza, az érintett érdekei és alapvető jogai elsőbbséget élveznek-e az adatkezelő érdekével szemben, figyelembe véve az adatkezelővel való kapcsolata alapján az észszerű elvárásait.

A jogos érdek fennállásának megállapításához körültekintően meg kell vizsgálni többek között azt, hogy az érintett a személyes adatok gyűjtésének időpontjában és azzal összefüggésben számíthat-e észszerűen arra, hogy adatkezelésre az adott célból kerülhet sor. Az érintett érdekei és alapvető jogai elsőbbséget élvezhetnek az adatkezelő érdekével szemben, ha a személyes adatokat olyan körülmények között kezelik, amelyek közepette az érintettek nem számítanak további adatkezelésre.

Az adatkezelő más jogalapon történő adatkezelés mellett is elvégezheti az érdekmérlegelési tesztet az érintettek magánszférájának arányos korlátozása érdekében.

2.8. Adatközlés, adattovábbítás, nyilvánosságra hozatal

Adattovábbítás az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele.

A Szervezet az érintettek személyes adatainak továbbítását az egyes adatkezelések tekintetében, kizárólag jelen szabályzatban meghatározottak alapján és feltételek szerint valósítja meg.

Harmadik fél részére adatot csak akkor továbbíthat, ha az alábbi feltételek közül legalább egy megvalósul:

- az érintett ehhez az adatkezelés során előzetesen hozzájárulását adta és ha az adatkezelés feltételei minden egyes adatra nézve teljesülnek;
- a törvény az adattovábbítást megengedi és az adatkezelés feltételei minden egyes személyes adatra nézve teljesülnek;
- az adatkezelőre vonatkozó jogi kötelezettség teljesítése céljából szükséges;
- az adatkezelő vagy harmadik személy jogos érdekének érvényesítése céljából szükséges, és ezen érdek érvényesítése a személyes adatok védelméhez fűződő jog korlátozásával arányban áll;
- a nemzetbiztonság, a honvédelem és a közbiztonság védelme, a bűncselekmények üldözése céljából az arra hatáskörrel rendelkező nemzetbiztonsági szerveknek, nyomozó hatóságoknak, bíróságoknak, valamint egyéb bírósági és nyomozó szervek jogszerű megkeresése esetén átadhatók az adattovábbítási kérsben megjelölt adatok tekintetében.

Személyes adatot csak akkor hozhat nyilvánosságra, ha erre megfelelő jogalappal rendelkezik. A személyes adatokon is alapuló, de anonimizált statisztikai adatok szabadon nyilvánosságra hozhatók.

2.8.1. Adattovábbítás harmadik országokba

A Szervezet jelenleg nem továbbít személyes adatokat harmadik országokba vagy nemzetközi szervezetek részére. A Vezetőfelelős azért, amennyiben személyes adatoknak harmadik országba vagy nemzetközi

szervezet részére történő továbbítására kerülne sor, az érintett jogosult arra, hogy tájékoztatást kapjon a továbbításra vonatkozóan a megfelelő garanciákról. A személyes adatoknak az Unióból harmadik országbeli adatkezelőknek, adatfeldolgozóknak, egyéb címzetteknek vagy nemzetközi szervezetek részére történő továbbítása esetén nem sérülhet a természetes személyeknek az Unióban a Rendelettel biztosított védelem szintje, és annak fenn kell maradnia az ilyen személyes adatoknak az adott harmadik országból vagy nemzetközi szervezettől ezt követően ugyanazon vagy másik harmadik országbeli adatkezelőnek, adatfeldolgozónak vagy nemzetközi szervezetnek történő újbóli továbbítása esetén is.

A harmadik országokba és a nemzetközi szervezetekhez való továbbítás csak a Rendelet teljes betartása mellett hajtható végre. A továbbításra akkor kerülhet csak sor, ha az adatkezelő vagy az adatfeldolgozó – e rendelet egyéb rendelkezéseire is figyelemmel – teljesíti az harmadik országok vagy nemzetközi szervezeteknek történő adattovábbításra vonatkozó, e rendeletben meghatározott feltételeket.

Az lbtv. hatálya alá tartozó szervezeteknek az lbtv. 3. § (2) - (5) bekezdése bizonyos esetekben ad lehetőséget, hogy egyes elektronikus információs rendszereit Magyarország területén kívül üzemeltesse, illetve azokban külföldön végezzenek adatkezelést. Az adatkezelés kezdetét legalább 90 nappal megelőzően írásbeli kérelmet kell benyújtani a Hatóságnak (nem szükséges a hatóság engedélye, ha a külföldi adatkezelést vagy üzemeltetést nemzetközi szerződés írja elő).

A kérelemhez csatolni kell:

- az EGT tagállamaiban történő adatkezelés indokát,
- az EGT tagállamaiban kezelt adatok és adatbázisok leírását,
- azt, hogy az adatkezelő rendszer, valamint üzemeltetője nevesített-e, és az adatkezelés jogszabályi megfeleléséért felelős személy neve, beosztása, elérhetősége ismert-e,
- az adatkezelő rendszer technikai és technológiai leírását, ideértve a hardver- és szoftverkomponenseket is,
- az adatkezelő rendszer információbiztonságának ismertetését, a rendszerhez kapcsolódó, továbbá az üzemeltetőre vonatkozó belső szabályozásokat és utasításokat,
- a kötelezően lefolytatandó biztonsági rendszerfelülvizsgálat eredményét,
- a magyar információvédelmi szabályok megtartásáról szóló üzemeltetői nyilatkozatot,
- azt, hogy az üzemeltetés helyszínén illetékes hatóságok jogosultak-e a kezelt adatokba betekinteni.

2.9. Adatfeldolgozás, adatfeldolgozói garancianyújtás

A Szervezet a felelősségébe tartozóan végzett adatkezelési, adatfeldolgozási tevékenységekről nyilvántartást vezet a 2.2. fejezet szerint.

A Szervezet, mint adatkezelő:

Ha a Szervezet az adatkezelő (a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt határozza meg), de bizonyos adatkezelési tevékenységekhez adatfeldolgozó szolgáltatásait is igénybe veszi, kizárólag olyan közreműködőt (adatfeldolgozót) vehet igénybe, aki megfelelő garanciákat nyújt az adatkezelés Rendelet követelményeinek való megfelelését és az érintettek jogainak védelmét biztosító, megfelelő technikai és szervezési intézkedések végrehajtására vonatkozóan.

Az adatfeldolgozói tevékenységet végző közreműködőket az Adatkezelési nyilvántartásban kell nyilvántartani.

Az adatfeldolgozói szerződéseknek célszerűen az alábbiakat kell tartalmaznia:

- az adatkezelő és az adatfeldolgozó személyét, elérhetőségét, ha az adatfeldolgozó rendelkezik Adatvédelmi tisztviselővel, annak elérhetőségét,
- az adatfeldolgozás jellegét, célját, időtartamát,
- az adatfeldolgozással érintett adatalanyok kategóriáit, a személyes adatok típusát, körét, mennyiségét,
- az adatfeldolgozó jogainak és kötelezettségeinek meghatározását, különösen annak rögzítését, hogy az adatfeldolgozó az adatkezelő kifejezett írásos utasításai alapján végezhet adatkezelési műveleteket, továbbá az esetlegesen bekövetkező adatvédelmi incidensek esetén követendő szabályok meghatározását,
- az elvégzett technikai műveletek megnevezését, módját,
- a feldolgozott személyes adatok további sorsát,
- annak rögzítését, hogy az adatfeldolgozó további adatfeldolgozót vehet-e igénybe,
- az adatkezelőt és az adatfeldolgozót terhelő technikai és szervezési intézkedések meghatározását, ezek igazolását az adatfeldolgozó részéről,
- az adatfeldolgozó azon alkalmazottai titoktartására vonatkozó rendelkezéseket, akik az adatfeldolgozásban részt vesznek,
- annak szabályozását, hogy az adatfeldolgozó milyen módon, eljárási rendet követve nyújt segítséget az érintettek jogait érintő kérelmek megválaszolásában,
- az adatkezelő ellenőrzési jogkörének biztosítását,
- az adatkezelő utasításadási rendjének meghatározását, beleértve az adatfeldolgozó azon kötelezettségét, hogy tájékoztassa az adatkezelőt, ha az adatkezelő által adott utasítás GDPR vagy egyéb vonatkozó jogszabályba ütközik,
- minden olyan információ adatkezelő rendelkezésre bocsátását, amely meghatározott kötelezettségek teljesítésének igazolásához szükséges, amely lehetővé teszi és elősegíti az adatkezelő által vagy az általa megbízott más ellenőr által végzett auditokat, beleértve a helyszíni vizsgálatokat is,
- az adatkezelési szolgáltatás nyújtásának befejezését követő eljárást (pl. az adatkezelő döntése alapján minden személyes adatot töröl, vagy visszajuttat, és törli a meglévő másolatokat, kivéve, ha az uniós vagy a tagállami jog a személyes adatok tárolását írja elő).

A Szervezet mint adatfeldolgozó:

A Szikszói Közös Önkormányzati Hivatal adatfeldolgozó tevékenysége során (ha van) az adatokat kizárólag az adatkezelő utasításának megfelelően kezeli, kivéve, ha az ettől való eltérésre uniós vagy tagállami jog kötelezi.

A feladatok ellátásához megfelelő ismerettel és gyakorlattal rendelkező személyeket vesz igénybe. Biztosítja, hogy az érintett személyes adatokhoz való hozzáférésre feljogosított személyek – ha jogszabályon alapuló megfelelő titoktartási kötelezettség hatálya alatt egyébként nem állnak – az általuk megismert személyes adatok vonatkozásában titoktartási kötelezettséget vállaljanak.

A tudomány és technológia állása és a megvalósítás költségei, továbbá 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 érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja.

Az adatkezelő előzetesen írásban tett eseti vagy általános felhatalmazása nélkül további adatfeldolgozót nem vesz igénybe. Az általános írásbeli felhatalmazás esetén tájékoztatja az adatkezelőt minden olyan tervezett változásról, amely további adatfeldolgozók igénybevételét vagy azok cseréjét érinti, ezzel biztosítva lehetőséget az adatkezelőnek arra, hogy ezekkel a változtatásokkal szemben kifogást emeljen.

Ha bizonyos, az adatkezelő nevében végzett konkrét adatkezelési tevékenységekhez további adatfeldolgozó szolgáltatásait is igénybe veszi, uniós vagy tagállami jog alapján létrejött szerződés vagy más jogi aktus útján erre a további adatfeldolgozóra is ugyanazok az adatvédelmi kötelezettségeket kell telepíteni, mint amelyek az adatkezelő és az adatfeldolgozó között létrejött szerződésben vagy egyéb jogi aktusban szerepelnek.

A további adatfeldolgozónak megfelelő garanciákat kell nyújtania a megfelelő technikai és szervezési intézkedések végrehajtására, biztosítania kell, hogy az adatkezelés megfeleljen a Rendelet követelményeinek. Ha a további adatfeldolgozó nem teljesíti adatvédelmi kötelezettségeit, az őt megbízó adatfeldolgozó teljes felelősséggel tartozik az adatkezelő felé a további adatfeldolgozó kötelezettségeinek a teljesítéséért.

Az adatkezelés jellegének figyelembevételével megfelelő technikai és szervezési intézkedésekkel a lehetséges mértékben segíti az adatkezelőt abban, hogy teljesíteni tudja kötelezettségét az érintett jogainak gyakorlásához kapcsolódó kérelmek megválaszolása tekintetében.

Segíti az adatkezelőt kötelezettségei teljesítésében, figyelembe véve az adatkezelés jellegét és a rendelkezésére álló információkat.

Az adatkezelő rendelkezésére bocsát minden olyan információt, amely kötelezettségei teljesítésének igazolásához szükséges, lehetővé teszi és elősegíti az adatkezelő által vagy az általa megbízott más ellenőr által végzett auditokat, beleértve a helyszíni vizsgálatokat is.

Az adatkezelés biztonsága érdekében meghatározott technikai, szervezési intézkedéseket az adatkezelővel kötött megállapodás tartalmazza, illetve a 4. fejezetben szerepelnek az adatkezelés során betartott intézkedések.

2.10. Kötelező adatkezelések felülvizsgálata

Az Infotv. 5.§ (3)-(5)bekezdése alapján az alábbi kötelező adatkezelések(Rendelet 6. cikk (1) c), e) pont) esetén a kezelendő adatok fajtáit, az adatkezelés célját és feltételeit, az adatok megismerhetőségét, az adatkezelő személyét, valamint az adatkezelés időtartamát vagy szükségessége időszakos felülvizsgálatát az adatkezelést elrendelő törvény, illetve önkormányzati rendelet határozza meg.

Ha a kötelező adatkezelés időtartamát vagy szükségessége időszakos felülvizsgálatát törvény, helyi önkormányzat rendelete vagy az Európai Unió kötelező jogi aktusa nem határozza meg, az adatkezelő az adatkezelés megkezdésétől legalább háromévente felülvizsgálja, hogy az általa, illetve a megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által kezelt személyes adat kezelése az adatkezelés céljának megvalósulásához szükséges-e.

Ezen felülvizsgálat körülményeit és eredményét az adatkezelő dokumentálja, e dokumentációt a felülvizsgálat elvégzését követő tíz évig megőrzi és azt a Nemzeti Adatvédelmi és Információszabadság Hatóság kérésére rendelkezésére bocsátja.

A Szikszói Közös Önkormányzati Hivatal a GDPR Reg Adatkezelési rendszerben végzi el és dokumentálja az adatkezelések felülvizsgálatát az egyes adatkezelésekre beállított felülvizsgálati gyakorisággal.

2.11. Adatvédelmi hatásvizsgálat

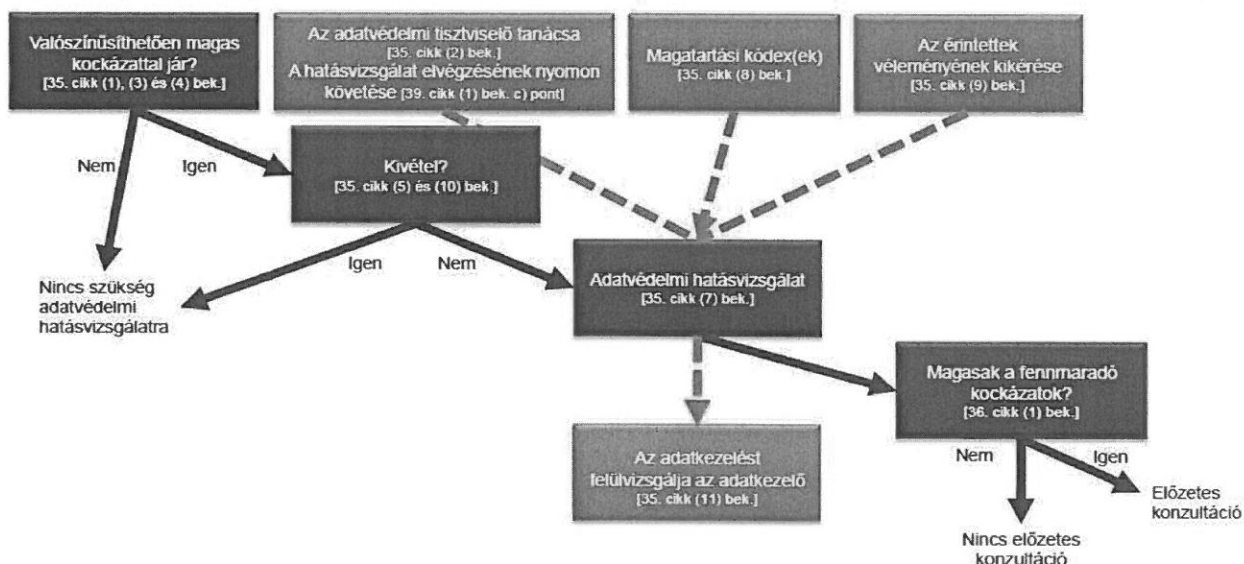
A természetes személyek jogaira és szabadságaira nézve magas kockázattal járó esetekben az adatkezelő – annak érdekében, hogy az adatkezelés jellegét, hatókörét, körülményeit és céljait, valamint a kockázat forrásait figyelembe véve felmérje a magas kockázat különös valószínűségét és súlyosságát – az adatkezelés előtt adatvédelmi hatásvizsgálatot végez arra vonatkozóan, hogy a tervezett adatkezelési műveletek a személyes adatok védelmét hogyan érintik. Ez magában foglalja különösen az említett kockázat mérséklését, a személyes adatok védelmét, a Rendeletnek való megfelelés bizonyítását célzó tervezett intézkedéseket, garanciákat és mechanizmusokat.

Az adatvédelmi hatásvizsgálatot az alábbi esetekben kell elvégezni:

- természetes személyekre vonatkozó egyes személyes jellemzők olyan módszeres és kiterjedt értékelése, amely automatizált adatkezelésen – ideértve a profilalkotást is – alapul, és amelyre a természetes személy tekintetében joghatással bíró vagy a természetes személyt hasonlóképpen jelentős mértékben érintő döntések épülnek,
- különleges adatok nagy számban történő kezelése,
- nyilvános helyek nagymértékű, módszeres megfigyelése,
- minden olyan adatkezelés tekintetében, amelyek valószínűsíthetően magas kockázattal járnak az érintettekre nézve.

A hatásvizsgálat kiterjed legalább:

- a tervezett adatkezelési műveletek módszeres leírására és az adatkezelés céljainak ismertetésére (beleértve adott esetben az adatkezelő által érvényesíteni kívánt jogos érdeket);
- az adatkezelés céljaira figyelemmel az adatkezelési műveletek szükségességi és arányossági vizsgálatára;
- az érintett jogait és szabadságait érintő kockázatok vizsgálatára; és
- a kockázatok kezelését célzó intézkedések bemutatására (a személyes adatok védelmét, és a Rendelettel való összhang igazolását szolgáló, az érintettek és más személyek jogait és jogos érdekeit figyelembe vevő garanciákra, biztonsági intézkedésekre, mechanizmusokra.



Az adatvédelmi hatásvizsgálatot a kijelölt felelős(ök) végzi(k) el, szükség szerint be kell vonni az érintett vezetőket, felelősöket (pl. informatikai, informatikai biztonsággal foglalkozó felelősöket). Az Adatvédelmi tisztviselő szakmai tanácsát ki kell kérni, a döntés során figyelembe kell venni.

A 2018. május 25-e előtt megkezdett és hatásvizsgálat elvégzését igénylő adatkezelések esetén az Infotv. 75.§ (3) bekezdése alapján legkésőbb 2021. május 25-ig végre kell hajtani a vizsgálatot, illetve azonnal, amennyiben az adatkezelés körülményeiben lényeges változás következik be.

A Szervezet, mint adatkezelő szükség szerint, de legalább az adatkezelési műveletek által jelentett kockázat változása esetén ellenőrzést folytat le annak értékelése céljából, hogy a személyes adatok kezelése az adatvédelmi hatásvizsgálatnak megfelelően történik-e.

Nem szükséges elvégezni a hatásvizsgálatot azokra az adatkezelési műveletekre, melyek jogalapját uniós vagy az adatkezelőre alkalmazandó tagállami jog írja elő, és e jog a szóban forgó, e jogalap elfogadása során egy általános hatásvizsgálat részeként már végeztek adatvédelmi hatásvizsgálatot (kivéve ha a tagállamok az adatkezelési tevékenységet megelőzően ilyen hatásvizsgálat elvégzését szükségesnek tartják).

Olyan egymáshoz hasonló típusú adatkezelési műveletek, amelyek egymáshoz hasonló magas kockázatokat jelentenek, egyetlen hatásvizsgálat keretei között is értékelhetők.

A hatásvizsgálat szükségességének megállapítását dokumentálni kell, a vizsgálat során figyelembe kell venni a felügyeleti hatóság által összeállított adatkezelések jegyzékét.

A Szikszói Közös Önkormányzati Hivatal az egyes adatkezelésekre vonatkozóan az adatvédelmi hatásvizsgálat szükségességét, a természetes személyek jogaira és szabadságára nézve valószínűsíthető kockázatokat a GDPR Reg Adatkezelési rendszerben vizsgálja meg a NAIH által összeállított adatkezelési műveletek típusainak a jegyzéke alapján, az adatkezelő által figyelembe vett egyéb szempontok figyelembevételével.

A Szervezet a hatásvizsgálatok lefolytatásánál figyelembe veszi, hogy a kockázati tényezők azonosításában nagy szerepe lehet az érintettek érdekeinek mérlegelése során az érintettekkel való konzultációnak. Az érintetti vélemények kikérése, beépítése, dokumentálása javasolt, ennek hiányát indokolni kell.

Ha az adatvédelmi hatásvizsgálat megállapítja, hogy az adatkezelés az adatkezelő által a kockázat mérséklése céljából tett intézkedések hiányában valószínűsíthetően magas kockázattal jár, a személyes adatok kezelését megelőzően konzultáció szükséges a felügyeleti hatósággal.

A Szikszói Közös Önkormányzati Hivatal a hatásvizsgálatot igénylő egyes adatkezelésre vagy az egymáshoz hasonló típusú, hasonló magas kockázatú adatkezelési műveletek esetén azok csoportjára az adatvédelmi kockázatok felmérését és a megfelelő kockázatkezelést, az intézkedések végrehajtását a GDPR Reg Adatkezelési rendszerben is elvégezheti és dokumentálhatja.

3. Személyes adatok kezelése, nyilvántartása

3.1. Munkavállalók adatkezelései

A Szervezet minden munkavállalójának (mint érintett természetes személy) személyes adatainak kezeléséért a Szervezet vezetője a felelős, aki biztosítja, hogy a munkaviszonyhoz, kormányzati szolgálati jogviszonyhoz vagy egyéb foglalkoztatásra irányuló jogviszonyhoz (továbbiakban jogviszonyhoz) kapcsolódóan folytatott adatkezelési műveletekre vonatkozóan, valamint az adatfeldolgozók részére átadott

adatok kapcsán az adatfeldolgozókkal is betartatja a Rendelet előírásait és a munkahelyi adatkezelések alapvető követelményeit.

A munkavállaló személyiségi joga akkor korlátozható, ha a korlátozás a jogviszony rendeltetésével közvetlenül összefüggő okból feltétlenül szükséges és a cél elérésével arányos. A személyiségi jog korlátozásának módjáról, feltételeiről és várható tartamáról, továbbá szükségességét és arányosságát alátámasztó körülményekről a munkavállalót előzetesen írásban tájékoztatni kell. A munkáltatónak szükségességi-arányossági tesztet kell végeznie, amely alapján igazolja a személyiségi jog korlátozásának jogszerűségét és azt, hogy az adatkezelés nem indokolatlan beavatkozás a munkavállaló magánszférájába.

Az érintett személy számára a munkáltató feladata az adatkezelés megkezdése előtt egyértelmű és részletes tájékoztatást adni az adatai kezelésével kapcsolatos minden jelentős tényről.

A Szikszói Közös Önkormányzati Hivatala munkavállalók adatkezelési tájékoztatóit a GDPR Reg Adatkezelési rendszerben készíti el az előzetesen egyedileg összeállított, folyamatosan aktualizált adatkezelések adataival a személyre szabott tájékoztatáshoz. A munkavállalói adatkezelési tájékoztatót tudomásulvétel igazolása céljából aláíratatja, archiválja vagy helyben szokásos és általában ismert módon közzéteszi.

A hozzájárulás alapján történő adatkezelés

A hozzájárulás egy vagy több célra jogalapon történő adatkezelés esetén az érintett munkavállaló írásbeli hozzájárulását adja személyes adatainak egy vagy több konkrét célból történő kezeléséhez. A jelenlegi joggyakorlat alapján munkaviszonyban a munkavállaló hozzájárulása az esetek döntő többségében a jogviszony függelmi jellege miatt nem lehet önkéntes, mert egyfajta egyensúlytalanság, hatalmi viszony áll fent a munkáltató javára. Hozzájárulásra, mint jogalapra, a munkahelyi adatkezelések esetében csak kivételesen lehet hivatkozni, alapvetően akkor, amikor egyértelmű, hogy az adatkezelés során feltétel nélküli „előnyöket” szerez a munkavállaló, és nem érheti őt semmilyen hátrány a hozzájárulás megtagadása esetén (ebben az esetben dokumentált előzetes tájékoztatás után egy tényleges szöveges, magyarázattal ellátott hozzájárulás aláírásával lehet bizonyítani a munkavállaló önkéntességét, megadva a lehetőséget a nemleges válaszra is). Egy hozzájárulás egy adatkezelési cél érdekében végzett adatkezeléshez való hozzájárulást jelenti. Több adatkezelési cél esetén több önkéntes, egyértelmű érintetti hozzájárulás szükséges.

Adatkezelés munkáltatói jogos érdek alapján, munkáltatói ellenőrzések

A Szikszói Közös Önkormányzati Hivatal, mint adatkezelőnek a munkavállalókkal kapcsolatosan, azoknak a fennálló jogviszonya alatt, illetve azt megelőzően és azt követően is fűződhet érdeke személyes adatok kezeléséhez. Adatkezelő vagy valamely harmadik fél jogos érdeke jogalapot teremthet az adatkezelésre, feltéve, hogy az érintett érdekei, alapvető jogai és szabadságai nem élveznek elsőbbséget, figyelembe véve az adatkezelővel való kapcsolata alapján az érintett észszerű elvárásait. Munkáltató a jogos érdek fennállásának megállapításához érdek mérlegelést végez, melynek során azt kívánja eldönteni, hogy az érintett magánszemély személyhez fűződő jogait az adatkezelés milyen mértékben korlátozza, az érintett érdekei és alapvető jogai elsőbbséget élveznek-e az adatkezelő érdekével szemben.

A Szikszói Közös Önkormányzati Hivatala jogos érdeke fennállásának megállapításához szükséges érdek mérlegelést a GDPR Reg Adatkezelési rendszerben dokumentálja. Az Érdék mérlegelés – Jogos

érdek vizsgálata dokumentumot az elszámoltathatóság, bizonyíthatóság érdekében aláírva archiválja és megismerteti az érintettekkel.

A Szervezet vezetője, mint munkáltató felelős azért, hogy az adatkezelés célját minden esetben világosan és egyértelműen határozza meg, a szükségesség-arányosság elvének megfelelően, az alkalmazott eszköz alkalmas legyen a megfogalmazott adatkezelési cél elérésére, csak szükséges mértékű adatkezeléssel járjon, és ellenőrzés csak a munkavégzéssel összefüggésben történjen, és soha nem irányuljon a munkavállalók emberi méltóságának a sérelmére, így a munkavállalók megfélemlítésére, megalázására, zaklatására, zavarására. A munkavállaló magánszférája meg kell, hogy maradjon. A munkavállalókat a munkahelyen is megilleti a magánélethez való jog, amelyeknek tipikus színterei: ebédlő, öltöző, pihenő helyiség, mosdók.

A munkavállaló a munkáltató által a munkavégzéshez biztosított számítástechnikai eszközt – eltérő megállapodás, rendelkezés hiányában – kizárólag a jogviszony teljesítése érdekében használhatja, tilos a munkahelyi infrastruktúra magán használatára.

A munkavállaló a jogviszonnyal összefüggő magatartása körében ellenőrizhető, akár technikai eszköz alkalmazásával is. Munkáltató kötelezettsége, hogy munkáltatói rendelkezéseinek, egyéb szabályoknak, pl. az informatikai biztonságra vonatkozó követelményeknek, munkavállalói kötelezettségeknek a betartását ellenőrizze, a fokozatosság elvének betartásával. A munkáltató ellenőrzése során a jogviszony teljesítéséhez használt számítástechnikai eszközön tárolt, a jogviszonnyal összefüggő adatokba tekinthet be. Olyan mélységben tekinthet be, amíg el nem tudja dönteni, hogy az adat magáncélú-e. Amennyiben igen, nem tekinthet be az adatokba.

Adatkezelő vagy harmadik fél jogos érdeke érvényesítéséhez szükséges jogalap szerinti adatkezelések lehetnek pl. a következők: munkahelyi megfigyelő rendszer, munkáltató által biztosított informatikai eszközök, gépjármű adatainak ellenőrzése, munkáltatói e-mail cím/fiók, internet és wifi használatának ellenőrzése, stb. (az aktuális Adatkezelési tájékoztató szerint).

3.2. Ügyfelekkel, szakfeladatokkal kapcsolatos adatkezelések

Az ügyfelekkel és szakfeladatokkal kapcsolatos adatkezelések is akkor jogszerűek, ha 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.

Közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges adatkezelés:

Ha az adatkezelésre közérdekű feladat végrehajtásához, illetve közhatalmi jogosítvány gyakorlásához szükséges, az adatkezelésnek az uniós jogban vagy valamely tagállam jogában foglalt jogalappal kell rendelkeznie, egyetlen jogszabály szolgálhat jogalapul több adatkezelési művelethez. Az adatkezelés célját uniós vagy tagállami jogban kell meghatározni, melyek pontosíthatják az adatkezelő megjelölésére vonatkozó szabályokat, az adatkezelés tárgyát képező személyes adatok típusát, az érintetteket, azokat a szervezeteket, amelyekkel a személyes adatok közölhetők, az adatkezelés céljára vonatkozó korlátozásokat, az adattárolás időtartamát, valamint egyéb, a jogszerű és tisztességes adatkezelés biztosításához szükséges intézkedéseket is meghatározhatják.

A Szikszói Közös Önkormányzati Hivatalaz érintettek tájékoztatóit a GDPR Reg Adatkezelési rendszerben készíti el az előzetesen egyedileg összeállított, folyamatosan aktualizált adatkezelések adataival.

A szerkeszthető adatkezelési tájékoztatók kategóriánként generálhatók, abból a célból, hogy adatkezelő személyre szabott tájékoztatóval tudja tájékoztatni az érintetteket (készülnek munkavállalói, ügyfelekkel kapcsolatos, és szakmai, valamint egyedileg létrehozott kategóriával kapcsolatos adatkezelési tájékoztatók, ha vannak), azok tartalmazzák az érintettek tájékoztatására szolgáló valamennyi rendelkezésre álló információt.

Az Ügyfelekkel kapcsolatos aktuális adatkezelési tájékoztató honlapon kerül publikálásra, ennek megkönnyítésére lehetséges a tájékoztatót tartalmazó weboldal domain nevéhez egyedi ún. API kód generálása. A weboldalt üzemeltető által elvégzett egyszeri kódbeillesztést követően automatikusan megjelenik a weboldalon a Szervezet ügyfelekkel kapcsolatos aktuális adatkezelési tájékoztatója.

3.2.1. Okmánymásolás

Adatkezelésnek minősül a személyes adatokon vagy adatállományokon végzett bármely művelet vagy műveletek összessége, így az adathordozóról készült másolatkészítés vagy a másolatoknak a bekérése is. Az adatkezelések során figyelembe kell venni az adattakarékosság és a célhoz kötött adatkezelés elvét, a személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból, és az adatok kezelése csak e célokkal összeegyeztethető módon történhet, a kezelt adatoknak az adatkezelési cél szempontjából megfelelőnek és relevánsnak kell lenniük, és a kezelt adatok körét a szükségesre kell korlátozni.

Az okmánymásolás csak akkor tekinthető jogszerűnek, ha az általuk gyűjtött adatok kezelésének szükségszerűségét az adatkezelő bizonyítani tudja. A bemutatott érvényes, személyazonosító okmányban szereplő személyazonosító adatokat a dokumentum közhiteles voltára tekintettel másolatkészítés nélkül is el kell fogadni. A személyazonosság igazolására alkalmas hatósági igazolványról készített másolat nem rendelkezik bizonyító erővel arról, hogy hiteles másolata egyérvényes hatósági okmánynak, és nem alkalmas a személyazonosság megállapítására sem. A fényképes igazolvány személyazonosítás céljából való bemutatása felel meg a hatályos jogszabályi rendelkezéseknek, a másolatok kezelése nem felel meg a célhoz kötöttség és az adattakarékosság követelményének. A bemutatott és az adatkezelő ügyintézője, munkatársa által szemrevételezett okmányokból rögzített személyes adatok helyességének utólagos ellenőrizhetősége önmagában nem tekinthető olyan jognak vagy kötelezettségnek, amely az adatkezelés jogszerűségét igazolhatná. A bemutatott érvényes hatósági igazolványokban szereplő adatokat a dokumentumok közhiteles voltára tekintettel másolatkészítés nélkül is el kell fogadni.

Technikai és szervezési intézkedések

A Szikszói Közös Önkormányzati Hivatal vezetője felelős azért, hogy figyelembe véve a szervezet méretét, a folyamatok bonyolultságát és kölcsönhatását, a személyzet kompetenciáját, valamint a vonatkozó törvényeket, előírásokat, elvárásokat, meghatározza informatikai- és adatbiztonsági követelményrendszerét és környezetét.

Jelen Adatvédelmi és adatbiztonsági szabályzat jóváhagyásával és hatályba léptetésével biztosítja, hogy az irányítása alatt eljáró, a személyes adatokhoz hozzáféréssel rendelkező természetes személyek kizárólag az utasításának megfelelően kezelhessék az említett adatokat, kivéve, ha az ettől való eltérésre uniós vagy tagállami jog kötelezi őket.

Elkötelezett, hogy a tudomány és technológia állása és a megvalósítás költségei, továbbá 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 hajtson végre annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja.

A Szikszói Közös Önkormányzati Hivatal az egyedi adminisztratív, fizikai és logikai védelmi intézkedéseket az alábbiakban határozza meg, erőforrásainak megfelelően törekszik a betartásukra, betartatásukra:

3.3. Adminisztratív védelmi intézkedések

- A Szervezet feladata a személyes adatokhoz, személyes adatokat tartalmazó dokumentumokhoz, az elektronikus információs rendszerhez hozzáféréssel rendelkező személyek (beleértve a külső személyeket, pl. üzemeltetőket is) folyamatos oktatásának, képzésének elősegítése, az ajánlott elektronikus információbiztonsági eljárások, technikák és technológiák naprakészen tartása. Cél, hogy a felhasználók tudatában legyenek az adatvédelmi és információbiztonsági elvárásoknak és fenyegetettségeknek, illetve felelősségeiknek (pl. jelentési kötelezettségüknek). A biztonság tudatosítása a felhasználók esetében oktató anyagok terjesztésével és képzések útján történik.
- Megismerteti és betartatja munkavállalóival, szerződéses partnereivel, harmadik felekkel - akik hozzáférnek személyes adatokhoz - a személybiztonsági eljárásrendet, szabályzatait, utasításait, az internethasználattal és az elektronikus levelezéssel, az elektronikus információs rendszerhez hozzáférési jogosultságot igénylő személyekkel, felhasználókkal szembeni elvárásokat, szabályokat, felelősségüket, az adott rendszerhez kapcsolódó kötelező, vagy tiltott tevékenységeket.
- Titoktartási nyilatkozat aláírására kötelezi őket, külső fél közötti jogviszony alapjául szolgáló megállapodásban rendelkezik a külső fél titoktartási kötelezettségéről.
- A jogviszony megszűnésekor az alkalmazottnak, bármely jogviszony alapján foglalkoztatottnak, szerződőnek, harmadik félnek az információkhoz és információ-feldolgozó eszközökhöz való hozzáférési jogosultságát megszünteti, visszaveszi az érintett személynek kibocsátott egyéni hitelesítő, hitelesítésre szolgáló eszközöket, felhasználói kártyákat, belépésre jogosító kártyákat (ha vannak), amikor alkalmazásuk megszűnik, szerződésük, illetve megállapodásuk lejár.
- Gondoskodik arról, hogy a tárolt adatokhoz belső rendszeren keresztül vagy közvetlen hozzáférés útján kizárólag az arra feljogosított személyek, kizárólag az adatkezelés céljával összefüggésben férjenek hozzá.

- A felhasználókat tudatosítja, hogy a tőle elvárható gondossággal kell eljárnia az adatkezelés során. Meg kell akadályoznia a kapott hozzáférési jogokkal való visszaélést azáltal, hogy megőrzi a hozzáférési adatok titkosságát, a felhasználó elszámoltatható minden olyan tevékenységért, amelyet a saját felhasználói azonosítójával végzett, vagy végeztek.
- A szerepkörök és jogosultságok változtatását, változáskezelés keretében hajtja végre, és a szükséges dokumentumokat módosítja (pl. szerződésben meghatározott szerepkör, feladatok, jogok és kötelezettségek, munkaköri leírás).
- Olyan mentési megoldásokat alkalmaz, illetve működtet, amivel biztosítani tudja, hogy az informatikai eszközök sérülése, meghibásodása, adathordozókon tárolt adatok sérülése, használhatatlanná válása esetén, a kiesett informatikai szolgáltatás elfogadható időn belül visszaállítható, illetve az elveszett adatmennyiség mértéke még kezelhető szinten marad. Azon adatok esetén, amelyek hosszú távú megőrzéséért felelős, a mentéseknek alkalmasnak kell lenni az adatok jogszabályban előírt megőrzési idejének végéig történő visszaállítására.
- Alapvető biztonsági szabályokat határoz meg és tart be:
 - o Eltérő megállapodás hiányában tilos a munkavégzéshez biztosított információtechnológiai vagy számítástechnikai eszköz, rendszer, elektronikus levelezési rendszer használata, a tulajdonában lévő internet hálózat feladatellátáson kívüli használata.
 - o A tulajdonát képező levelező rendszer – engedélyezés hiányában – csak szervezeti célokra alkalmazható. Ha a felhasználó a postafiókjára elektronikus levélben vagy annak mellékletében kapott olyan állományt, amely nem munkavégzéshez kapcsolódik, azt haladéktalanul törölnie kell, a tulajdonában lévő adathordozókra tilos a munkavégzéshez nem kapcsolódó, személyes adatot tartalmazó dokumentum (beleértve a fényképeket is) mentése. A felhasználó felel valamennyi, a címéről elküldött levél rendeltetési helyéért és annak tartalmáért.
 - o Javasolt a felhasználóhoz kötött egyéni, teljes névvel ellátott, a szervezet által használt domain nevű egyedi e-mail-címek létrehozása (vezetéknév.keresztnev@domain.hu).
 - o Levelezés a meghatározott, lehetőleg a Szervezet saját tulajdonú domain névhez kapcsolódó tárhelyén történhet, a meghatározott vagy a tárhely szolgáltató által biztosított levelező rendszer használatával, az ingyenes levelezőrendszerek (pl. freemail, gmail, stb.) használatát lehetőleg technikai korlátozásokkal is tiltani kell. Az archív e-mail-ek elérését központi tárhelyen kell biztosítani.
 - o Tilos más postafiókjához felhatalmazás nélkül hozzáférni, más nevében elektronikus üzenetet küldeni, fogadni.
 - o A levelezési fiókhozzáférést biztosító jelszót a felhasználónak titkosan kell kezelni, azt mások tudomására hozni még a munkafolyamat felgyorsítása érdekében is tilos. Jelenteni kell a jelszavak nyilvánosságra kerülésére utaló minden gyanút és körülményt.
 - o Ha a felhasználó nem ismeri a külső rendszerből érkező levél feladóját, akkor az üzenet megnyitása előtt igyekezzen azt beazonosítani, gyanús esetben törölje az üzenetet, illetve jelezze ezt felettesének vagy a rendszergazdának. Amennyiben a megnyitás szükséges annak megállapítására, hogy mi az üzenet célja, úgy ezt megfelelő előrelátással (lehetőleg a belső hálózattól elszeparált számítógépen) tegye, és az esetleges csatolt melléklet megnyitását vírus veszély miatt feltétlenül kerülje, további címzettnek nem küldheti tovább.
 - o Tilos a tulajdonában álló informatikai hálózatán, eszközein a nem engedélyezett felhőszolgáltatás, nem szakmai letöltések, tiltott oldalak, nem kívánt levelezőlisták stb. használata, lánclevelek indítása vagy továbbítása, szerzői jogok megsértése (pl. szoftver nem jogszerű terjesztése), egyéni

profitszerzést célzó, a szervezettől eltérő üzleti célú tevékenység és reklám, a hálózat, a kapcsolódó hálózatok, illetve ezek erőforrásainak rendeltetésszerű működését és biztonságát megzavaró, veszélyeztető tevékenység, ilyen információknak és programoknak a terjesztése, a hálózat erőforrásaihoz, a hálózaton elérhető adatokhoz történő illetéktelen hozzáférés kísérlete, a hozzáférés átruházása más személy részére, a hálózat erőforrásainak, a hálózaton elérhető adatoknak illetéktelen módosítására, megromlására, megsemmisítésére vagy bármely károkozásra irányuló tevékenység, a Szervezettel kapcsolatos információk nyilvános internetes oldalakon való illegális közzététele.

- Tilos az elektronikus információs rendszerek biztonsági beállításainak megváltoztatása, illetve a vírusellenőrző és Internet böngésző beállítások módosítása.
 - A kijelölt személy rendszeresen ellenőrzi, hogy a felhasználók számára biztosított az Internet elérést lehetővé tevő szoftverek mentesek a komolyabb biztonsági hibáktól.
 - Az elektronikus levelekben, vagy azok mellékleteként a csatolt állományokat az informatikai rendszer automatikusan ellenőrzi, és a biztonságos üzemeltetést veszélyeztető állományok esetében a használatot, illetve a küldés/fogadást megakadályozza. Az állományok küldésére és fogadására vonatkozó korlátozás kiterjed a rendeltetésszerű- és az észszerű használat kereteit meghaladó méretű állományokra is.
- A Szervezet kötelezettsége, hogy munkáltatói rendelkezéseinek, egyéb szabályoknak, pl. az informatikai biztonságra vonatkozó követelményeknek, munkavállalói kötelezettségeknek a betartását ellenőrizze, ennek érdekében a felhasználók által böngészett oldalak listáját naplózhatja, az általa biztosított informatikai eszközöket, adathordozókat, munkáltatói e-mail-címet/fiókot, internet és wifi használatot ellenőrizheti, melynek célja, hogy a felhasználók Internet használata megfeleljen a biztonsági követelményeinek és jogos érdekeinek.
 - A felhasználót tájékoztatja, tudomásul veteti, hogy a Szervezet informatikai hálózatára, eszközeire vonatkozóan ellenőrzési és felelősségre vonási jogosultsága fennáll, a meghatározott viselkedési szabályok megsértése esetén, az adatvédelmi és elektronikus információbiztonsági szabályokat és az ehhez kapcsolódó eljárásrendeket megsértő személyekkel szemben belső eljárási rend szerint fegyelmi eljárást kezdeményez, illetve érvényesíti a vonatkozó szerződésben meghatározott következményeket, megvizsgálja és szükség szerint alkalmazza az egyéb jogi lépéseket.
 - Ha a tevékenység jellege, vagy jogszabályi követelmények megkövetelik, hogy rendelkezzen olyan tervekkel, melyek lehetővé teszik a rendeltetésszerű működéstől eltérő, rendkívüli helyzetek kezelését, akkor Ügymenet folytonossági tervet (BCP) készít, amelynek célja a legfontosabb (kritikus) folyamatok kiesési idejének minimalizálása, az informatikai rendszer normál állapotának lehető legrövidebb időn belül történő visszaállításán túl az, hogy ezt kockázatokkal arányosan lehessen megvalósítani. Ha szükséges, akkor Katasztrófa-elhárítási tervet készít, amely meghatározza a szervezet információs/informatikai rendszereinek teljes működésének (minden funkcionalitásának) a visszaállítását vagy újra felépítését.
 - A bemutatott hatósági okmányokról törvényi kötelezés alapján készít másolatot. A célhoz kötöttség és az adattakarékosság alapelvének érvényesülése érdekében, az okmány bemutatása mellett, az érintett általi nyilatkozat kitöltése vagy arról feljegyzés készítése, illetve a „négy szem elve” (egy másik ügyintéző is megnézi az érintett által bemutatott okmányt, és ő is megerősíti a személyazonosságot és a rögzített adatok pontosságát) által gyűjti be a szükséges adatokat. A Hatóság szerint kevésbé korlátozza a magánszférát egy feljegyzés készítése vagy egy nyilatkozat kitöltése, mint az okmányok másolása, a másolat készítése nem tekinthető a magánszféra arányos korlátozásának más, hasonlóan

hatékony intézkedésekhez képest. Kényelmi szempontok vagy „gyorsabb ügyintézés” nem indokolhatják a másolat készítését.

3.4. Fizikai védelmi intézkedések

- A Szikszói Közös Önkormányzati Hivatal az elektronikus információs rendszereket és az irattároló helyiségeit fizikailag védett, biztonságos helyre telepíti.
- Lehetőség szerint vagyonsvédelmi rendszerekkel, távfelügyeleti szolgáltató felügyeleti rendszerére csatlakozó riasztórendszerrel, ha jogos érdekei indokolják, akkor beléptetőrendszerrel, kamerarendszerrel) is védi az adathordozókat tartalmazó helyiségeit, eszközeit a jogosulatlan fizikai hozzáféréstől.
- Felügyelet alatt tartja az adathordozókat tartalmazó helyiségeket, ügyfelek, látogatók nem tartózkodhatnak kíséret nélkül.
- Alkalmazza az „Üres íróasztal - tiszta képernyő” szabályt:
 - o a monitorok elhelyezésekor törekszik az azokra való minél kisebb rálátás biztosítására, hogy a képernyők tartalma ne legyen olvasható az alkalmilag arra haladó személyek számára, és ne legyen látható az épületen kívülről (ha monitor elhelyezéssel nem biztosítható, akkor sötétítő függöny használatával);
 - o a felhasználó a számítógépét zárja, ha azt rövidebb időre őrizetlenül hagyja;
 - o a munkafázis végeztével vagy hosszabb idejű távollét esetén a számítógépből kijelentkezik, illetve kikapcsolja;
 - o törekszik arra, hogy munkavégzés után minden érzékeny információt tartalmazó anyagot (papír alapú anyagokat, valamint elektronikus adathordozókat) eltávolít az asztalokról és zárható irodabútorban tárol;
 - o gondoskodik arról, hogy a nyomtatókból, faxokból, fénymásolókból kijövő dokumentumokhoz illetéktelenek ne férjenek hozzá;
 - o ügyel arra, hogy érzékeny információt tartalmazó dokumentumok ne maradjanak a fénymásolóban, a kinyomtatott, faxolt vagy másolt dokumentumokat nem hagy őrizetlenül az eszközökben;
 - o a hibásan nyomtatott, nem használt dokumentumokat megsemmisít (pl. iratmegsemmisítővel).
- A fénymásoló és nyomtató berendezéseket/multifunkcionális nyomatkészítőket, a fax készülékeket és minden egyéb kimenteti eszközt védett területen belül helyezi el, ahol a felügyeletük biztosítható, az illetéktelen hozzáférés megakadályozható (harmadik fél, ügyfél és látogatók részére nem hozzáférhetőek), vagy nyilvános zónában PIN kóddal védett nyomtatás kerül beállításra.
- Védi a helyiségeit az adathordozókat károsító behatásoktól (extrém hőmérséklet és páratartalom), az informatikai erőforrásokat koncentráltan tartalmazó helyiségekben (pl. szerverhelyiség) szükség esetén biztosítja a megfelelő környezeti feltételeket.
- Az elsődleges áramforrás kiesése esetére azokhoz a rendszerekhez, ahol az indokolt vagy elvárt (pl. szerverfunkciójú számítógépek, adatmentő szerverek, hálózati eszközök), az eszközök szabályos leállításához a tevékenységhez méretezett, rövid ideig működőképes szünetmentes áramellátást biztosít.
- Azokban a helyiségekben, ahol az indokolt (pl. szerverszobában) független áramellátással támogatott észlelő berendezést (füstérzékelőt) alkalmaz, azok jelzéseit a vagyonsvédelmi rendszer részeként hatósági engedéllyel rendelkező távfelügyeleti szolgáltató felügyeleti rendszerére csatlakoztat.

- Az adatvesztés megelőzése érdekében betartja a tűzvédelmi előírásokat, az informatikai eszközök központi helyiségeibe (elosztó-, szerverhelyiségekbe) és ahol a tűzvédelmi szempontból indokolt, minimális elvárásként tanúsított gázzal oltó (CO₂) hordozható, kézi tűzoltó készülékeket biztosít.

3.5. Logikai védelmi intézkedések

- A Szikszói Közös Önkormányzati Hivatal kizárólag olyan szoftvereket és kapcsolódó dokumentációt használ, amelyek megfelelnek a rájuk vonatkozó szerződésbeli elvárásoknak és a szerzői jogi, vagy más jogszabályoknak.
- Szabályokhoz köti a szoftverek, alkalmazások telepítését, másolását, eltávolítását, a megfelelő biztonsági beállításokat.
- Betartja a hozzáférés ellenőrzési eljárásrendet, az elektronikus információs rendszer, rendszerelem használója kizárólag személy vagy szerződéses jogviszonyban álló szerződött partner, harmadik személy, aki a munkavégzéshez szükséges feltételekkel, megismerte a vonatkozó szabályokat, vonatkozó rendelkezéseket, és ennek megfelelően hozzáférési jogosultságot kapott az elektronikus információs rendszerek használatához.
- A hozzáférési jogosultságok megszüntetéséről szükség esetén intézkedik: kilépés, jogviszony megszűnése, szerződés lejáratát vagy megszűnése, kinevezés visszavonás, szervezeten belüli áthelyezés, munkakör jelentős megváltozása, tartós betegség, távollét, illetve helyettesítés esetén, valamint visszaélés gyanúja vagy hasonló súlyos biztonsági esemény felmerülése esetén.
- Biztosítja, hogy megfelelő jogosultság nélkül senki sem férhet hozzá a Szervezet rendszereihez, illetve olyan számítógépekhez, melyek ügyfél adatokat vagy bizalmas információt, védendő személyes adatokat tartalmaznak. Senki sem végezhet jogosulatlanul bármiféle változtatást az informatikai rendszerekben, beleértve az adatok törlését vagy megváltoztatását is.
- Az illetéktelen használat megakadályozására a munkaállomásokon automatikus képernyővédelmet állít be úgy, hogy felhasználói inaktivitást követően meghatározott időtartalom után automatikusan zárolja a munkaállomást. Az ismételt bejelentkezés kizárólag a felhasználó azonosításával és hitelesítésével történhet (felhasználónév és jelszó megadása).
- Kizárólag indokolt esetben engedélyezi a vezeték nélküli kapcsolaton keresztüli csatlakozást az elektronikus információs rendszeréhez, felhasználói korlátozásokat vezet be.
- Gondoskodik a felhasznált eszközök szükséges, rendszeres karbantartásáról, fejlesztéséről. A karbantartásokat és javításokat ütemezetten, dokumentáltan hajtja vagy hajtja végre.
- A karbantartásokat, javításokat csak az arra jogosult személyek végzik. Karbantartás céljából az adathordozók, információs rendszer vagy rendszerelem szállítását a rendszergazda, külső személy/szolgáltató esetében a megbízott személy/szolgáltató végzi.
- Gondoskodik arról, hogy a felhasználók, a felhasználók által végzett tevékenységek – az engedélyezett jogosultságoknak megfelelően – egyedileg legyenek azonosítva és hitelesítve, abból a célból, hogy elkerülhetővé váljanak a jogosulatlan hozzáférések, csökkenve a jogosulatlan hozzáférésekből származó információbiztonsági incidenseket.
- Kizárólag a tulajdonában lévő, nyilvántartott adathordozó, illetve behozott adathordozó esetében ellenőrzött és engedélyezett eszköz használatát engedélyezi.
- Az adathordozók használatát egyes informatikai eszközökön információbiztonsági megfontolásból utasítással, hardver, illetve szoftver úton korlátozhatja, figyelheti, monitorozhatja. Engedélyezheti, korlátozhatja vagy tilthatja bizonyos, vagy bármely adathordozó típusok használatát a kijelölt

elektronikus információs rendszereken vagy rendszerelemeken működő biztonsági intézkedések használatával.

- Írásos engedélyhez köti az adathordozók, mobil eszközök (laptop, pendrive, floppy, CD stb.) - otthoni vagy külső helyszínen történő munkavégzés, vagy bármilyen más célból történő - kiszállítását.
- Lehetőség szerint a mobil/szervezeten kívül kiszállításra engedélyezett hordozható eszközöket kriptográfiai (hardver vagy szoftver titkosítási) mechanizmusokkal is védi a digitális adathordozókon tárolt információk bizalmosságának és sértetlenségének védelme érdekében (hordozható adattároló, pl. okostelefon, laptop, pendrive stb.). A kiszállított mobil eszközök esetén eszköztitkosítást, tároló alapú titkosítást, vagy más technológiai eljárást alkalmaz (pl. BIOS jelszó, Win10 Pro esetén BitLocker, ESET EndpointEncryption). Kizárólag nyilvántartott, hardveres titkosítású pendrive használat engedélyezett.
- Betartatja az adattartalommal bíró adathordozók, információs rendszer vagy rendszerelem szállítása esetén a megfelelő információbiztonsági intézkedéseket. Karbantartás céljából az adathordozók, információs rendszer vagy rendszerelem szállítását a rendszergazda, külső személy/szolgáltató esetében a megbízott személy/szolgáltató végzi.
- Biztosítja, hogy az operációs rendszerek vagy üzletileg kritikus alkalmazások verziófrissítése megtervezett módon történjen meg, a biztonságkritikus szoftverek a frissítésük kiadását követő meghatározott időtartamon belül telepítésre kerüljenek (a frissítések történhetnek automatikusan is az adott operációs rendszer frissítési beállításainak megfelelően). Egyéb biztonsági kockázatot nem jelentő frissítéseket csak abban esetben telepíti, ha azok üzleti szempontból lényeges hibák, sérülékenységek kijavítását, funkcióbővítést eredményeznek.
- Meghatározta és betartatja az adathordozók kezelésének általános irányelveit:
 - o informatikai eszközöket, adathordozókat tilos nyilvános helyen vagy harmadik félnél történő munkavégzés során őrizetlenül hagyni;
 - o munkavégzés közben nem lehet a használatban lévő mobil eszközöket felügyelet nélkül hagyni, a használaton kívüli eszközöket védett helyen kell tárolni („tiszta asztal” szabálya);
 - o az informatikai infrastruktúra elemeit engedély nélkül, nem a munkaköri feladatba tartozó módon megváltoztatni, vagy eltávolítani nem lehet;
 - o tilos az olyan hordozható adathordozó használata az elektronikus információs rendszerben, melynek tulajdonosa nem azonosítható. Az adathordozókat sorszámmal és/vagy a felügyeletéért felelős nevével azonosítani kell, azokat a felhasználóhoz kell rendelni;
 - o az adathordozókat a felhasználók nem csatlakoztathatják egymás eszközeihez úgy, hogy az eszköz tulajdonosa nem tud róla;
 - o amennyiben kívülről érkezik adat valamilyen adathordozón, annak a megtekintése csak előzetes ellenőrzés és a vírus mentesség megállapítása után használható;
 - o bármely adathordozó eltűnését azonnal jelenteni kell a Szervezet vagy szervezeti egység vezetőjének, a továbbiakban az adatvédelmi incidensként kell kezelni a 2.6. fejezet szerint.
- Betartja az adathordozók törlésére vonatkozó biztonsági irányelveket:
 - o az adathordozókat elhasználódásuk esetén cserélni és selejtezni kell az adatvesztés elkerülése érdekében,
 - o az adathordozókat selejtezés, a szervezeti ellenőrzés megszűnte, vagy újrafelhasználásra való kibocsátás előtt dokumentáltan adatmentesíteni kell ilyen célú megfelelő alkalmazással,
 - o a nem törölhető adathordozókat meg kell semmisíteni iratmegsemmisítőben vagy más módon össze kell törni,

- a törlési mechanizmusokat az információ minősítési kategóriájával arányos erősségnek és sértetlenségnek megfelelően kell alkalmazni, biztosítva, hogy a megsemmisítési eljárások során az kimeneti információk tartalma helyreállíthatatlanul megsemmisüljön.
- Meghatározta és érvényesíti a felhasználó számítógépes szolgáltatásokhoz való hozzáférési jogosultságának hitelesítésére szolgáló jelszavak kezelésével kapcsolatos elvárásait:
 - a munkaadások, rendszerlemek, rendszerek hozzáféréséhez szükséges jelszavakat a jelszavak erősségének irányelve alapján kell megadni (figyelembe véve a jelszavak kompromittálásából adódó kockázatokat);
 - a jelszavak erősségének irányelve: a jelszavak minimális hossza 6 karakter, tartalmazniuk kell kis- és nagybetűket, speciális és numerikus karaktereket egyaránt. Tilos olyan jelszavakat alkalmazni, melyek könnyen kitalálhatóak, mint például a személyes adatok, egyértelmű dátumok, gépnévre vagy a felhasználói névre utalóak vagy általános, szótári szavak (pl. „admin”, „password”), illetve amelyek gyári beállítású, alapértelmezett jelszavak;
 - a munkaadásokhoz, rendszerlemekhez, információs rendszerekhez kiadott kezdő jelszavakat kötelező az első bejelentkezés alkalmával megváltoztatni;
 - a felhasználók és megbízott harmadik felek felelősek a személyes jelszavaik megfelelő védelméért és annak következményeiért, ha a jelszavaik mások által ismertté válnak;
 - a jelszavakat azonnal meg kell változtatni, ha a felhasználó úgy gondolja, hogy azok más tudomására jutottak, vagy valami szokatlan tapasztaltak a számítógépes rendszerükben (ezt követően értesíteni kell a rendszergazdát és az elektronikus információs rendszer biztonságáért felelős személyt);
 - a jelszavakat rendszeres időközönként cserélni kell (lehetőség szerint automatikusan kikényszerítve), illetve az elektronikus információs rendszer által kikényszerített, vagy az üzemeltetők által meghatározott időközönként;
 - új jelszónak nem szabad az utolsó 5 régebbi közül egyiket sem megadni;
 - a jelszavakat alapvetően tilos leírni;
 - nem tehető a jelszó egy automatikus bejelentkezési folyamat részévé;
 - tilos a felhasználóknak bejelentkezni olyan felhasználónévvel, melyet eredetileg nem nekik bocsátottak ki, és amelyek használatára nem jogosultak;
 - amennyiben a felhasználók által használt rendszerek valamelyike a fentieknél alacsonyabb biztonsági szintet követelne meg, a felhasználóknak minden esetben az itt szereplő szabályok szerint kell eljárni;
 - ez a jelszó politika érvényes azokra a külső rendszerekre is, amelyeket a felhasználók a munkájukkal kapcsolatosan elérnek.
- Amennyiben erre lehetőség van, a folyamatos ügymenet biztosítása érdekében beállítja az egyes informatikai rendszerekben a helyettesítéseket, vagy biztosítja, hogy az egyes rendszerekhez több felhasználónak legyen kiosztva jogosultsága.
- Törekszik a legkisebb jogosultság kiosztásához. Valamennyi felhasználó munkavégzése során a szükséges és elégséges hozzáférés elve alapján kizárólag a feladat ellátásához szükséges adat, információ megismerésére, továbbá az adat- és rendszerhozzáférésre a munkavégzéséhez szükséges lehető legrövidebb ideig és szükséges legkisebb jogosultsági szint alkalmazásával jogosult. A szükséges mértékre és időtartamra történő korlátozás nemcsak a hozzáférés kockázatát minimalizálja, hanem a hozzáférő személy által viselt felelősséget is.
- A hitelesítésre vonatkozó követelményeket valamennyi rendszerelemre vonatkozóan érvényesíti.

- A menedzselhető hálózati aktív eszköz tekintetében az eszköz gyári, alapértelmezett bejelentkezési azonosítóit (név, password) megváltoztatja. Csak előre kijelölt, privilegizált felhasználóknak van lehetősége bejelentkezni az eszközökbe.
- Megfelelő védelmi szoftverek és eszközök (tűzfal, vírusirtó) alkalmazásával és az alkalmazások biztonsági beállításával mindent megtesz a rosszindulatú programok károkozásával szemben.
- A munkaállomásokon lévő víruskeresőt úgy állítja be, úgy üzemelteti, hogy az automatikusan ellenőrizze a munkaállomásra csatlakoztatott adathordozókat, akadályozza meg a vírusok adathordozón, vezetékes vagy vezeték nélküli hálózaton, elektronikus levelezésben, vagy internet használat során történő bejutását a rendszerekbe, rendszeres ellenőrzéseket hajtson végre a belépési/kilépési pontokon, szükség esetén automatikusan riassza a rendszergazdát vagy a meghatározott további személyeket. Az esetlegesen mégis bejutott vírusok kártételének meggátítása céljából a rendszereket lehetőleg automatikusan, a felhasználó beavatkozását nem igénylő módon, rendszeresen át kell vizsgálni, és a bejutott kártékony kódokat meg kell semmisíteni.
- Megtiltja, hogy az elektronikus postafiókba érkező, ismeretlen feladótól származó, nem szokványos formátumú, gyanús csatolmányt tartalmazó, illetve idegen nyelvű küldemények, vagy a vírusvédelmi rendszer riasztása esetén bármely állomány, weboldal megnyitásra kerüljön.
- A szükséges mértékben naplózza a személyes adatok hozzáféréseit, valamint a biztonsági eseményeket.
- Szükség esetén belső engedélyhez köti az elektronikus információs rendszerek kapcsolódását más elektronikus információs rendszerekhez, dokumentálja az egyes kapcsolatokat, az interfészek paramétereit, a biztonsági követelményeket és a kapcsolaton keresztül átvitt elektronikus információk típusát.
- A saját hatókörben beszerzett rendszerekre, rendszerelemekre vonatkozóan az elektronikus információs rendszereinek teljes életútján, azok minden életciklusában figyelemmel kíséri informatikai biztonsági helyzetüket. Folyamatosan fel kell térképezni az összes üzemelő, használatban lévő vagy a jövőben bevezetésre tervezett informatikai eszközt, rendszert, a kezelt adatokat, a kezelt személyes adatokat és mindezek környezetét alkotó összes rendszerelemet (azok teljes életciklusában a tervezéstől, elkészítéstől, a rendszerből történő teljes kivonásáig, vagy megsemmisítésig).
- A legszűkebb funkcionalitás érdekében az elektronikus információs rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztője, illetve üzemeltetője az elektronikus információs rendszert úgy konfigurálja, hogy az csak a szükséges szolgáltatásokat nyújtsa.
- Saját hatókörén belül meghatározza és biztosítja azokat a minimum konfigurációs beállításokat, amelyek a munkavégzéshez szükségesek. Ennek köszönhetően, semmilyen felesleges beállítás, plusz szolgáltatás/funkció nem kerül konfigurálásra.
- Korlátozza egyes szoftverek és szolgáltatások hozzáférését. Tiltja egyes portok, protokollok elérhetőségét elkerülve ezzel a külső támadásokat. Szükséges mértékben korlátozza a külső portok (pl. usb) használatát.

4.4. Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény hatálya alá tartozó szervek további követelményei

Az lbtv. hatálya alá tartozó állami és önkormányzati szervezeteknek teljesíteni kell a 2013. évi L. törvény, valamint a törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet Védelmi intézkedések fejezetben felsorolt, az informatikai rendszerek biztonsági osztályához tartozó adminisztratív, fizikai és logikai védelmi intézkedéseket, illetve a központi szolgáltató (a jogszabály által kijelölt központosított informatikai és elektronikus hírközlési szolgáltató) előírásait. A betartandó követelményeket az *Informatikai biztonsági szabályzat* tartalmazza részletesen.

Az elektronikus információs rendszer biztonságáért felelős személy felel a Szervezetnél előforduló valamennyi, az elektronikus információs rendszerek védelméhez kapcsolódó feladat ellátásáért.

Az lbtv. 3. § (2) -(3) bekezdése alapján a külföldi adatkezelést, az egyes elektronikus információs rendszerek Magyarország területén kívül üzemeltetését előzetesen engedélyeztetni kell (pl. honlap üzemeltetés, email szerver).Lásd 2.8.1. *Adattovábbítás harmadik országokba* fejezetet.

Fogalomtár

A meghatározások megfelelnek az Európai Parlament és a Tanács (EU) 2016/679 rendeletében és az információs önrendelkezési jogról és információszabadságról szóló 2011. évi CXII. törvényben használt kifejezéseknek:

adatállomány: az egy nyilvántartásban kezelt adatok összessége;

adatfeldolgozás: az adatkezelő megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által végzett adatkezelési műveletek összessége;

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

adatfelelős: az a közfeladatot ellátó szerv, amely az elektronikus úton kötelezően közzéteendő közérdekű adatot előállította, illetve amelynek a működése során ez az adat keletkezett;

adatkezelés korlátozása: a tárolt személyes adatok megjelölése jövőbeli kezelésük korlátozása céljából;

adatkezelés: a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés;

adatkezelő: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza (15810908); ha az adatkezelés céljait és eszközeit az uniós vagy a tagállami jog határozza meg, az adatkezelőt vagy az adatkezelő kijelölésére vonatkozó különös szempontokat az uniós vagy a tagállami jog is meghatározhatja;

adatközlő: az a közfeladatot ellátó szerv, amely – ha az adatfelelős nem maga teszi közzé az adatot – az adatfelelős által hozzá eljuttatott adatot honlapon közzéteszi;

adatmegsemmisítés: az adatot tartalmazó adathordozó teljes fizikai megsemmisítése;

adattovábbítás: az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele;

adattörlés: az adat felismerhetetlenné tétele oly módon, hogy a helyreállítása többé nem lehetséges;

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;

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;

azonosítható természetes személy: az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, azonosító szám, helymeghatározó adat, online azonosító vagy a természetes személy fizikai, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható;

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 2016.5.4. L 119/33 Az Európai Unió Hivatalos Lapja HU 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;

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;

érintett hozzájárulása: az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez;

érintett: bármely információ alapján azonosított vagy azonosítható természetes személy;

felügyeleti hatóság: egy tagállam által az 51. cikknek megfelelően létrehozott független közhatalmi szerv. Magyarországon a NAIH (Nemzeti Adatvédelmi és Információszabadság Hatóság), mint az Infotv. által 2012. január 1-vel létrehozott, az adatvédelmi biztos intézményét felváltó nemzeti adatvédelmi hatóság. Feladata a két információs jog védelme és a magyarországi adatkezelések törvényességének felügyelete;

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;

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;

harmadik ország: minden olyan állam, amely nem EGT-állam;

hozzájárulás: az érintett akaratának önkéntes, határozott és megfelelő tájékoztatáson alapuló egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy az akaratát félreérthetetlenül kifejező más magatartás útján jelzi, hogy beleegyezését adja a rá vonatkozó személyes adatok kezeléséhez;

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

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;

közérdekből nyilvános adat: a közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli;

közérdekű adat: az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő és tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől, így különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre, annak eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat;

közös adatkezelő: az az adatkezelő, aki vagy amely – törvényben vagy az Európai Unió kötelező jogi aktusában meghatározott keretek között – az adatkezelés céljait és eszközeit egy vagy több másik adatkezelővel közösen határozza meg, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket egy vagy több másik adatkezelővel közösen hozza meg és hajtja végre vagy hajtja végre az adatfeldolgozóval;

közvetett adattovábbítás: személyes adatnak valamely harmadik országban vagy nemzetközi szervezet keretében adatkezelést folytató adatkezelő vagy adatfeldolgozó részére továbbítása útján valamely más harmadik országban vagy nemzetközi szervezet keretében adatkezelést folytató adatkezelő vagy adatfeldolgozó részére történő továbbítása;

különleges adat: a személyes adatok különleges kategóriába tartozó minden adat, azaz a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a genetikai adatok, a természetes személyek egyedi azonosítását célzó biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok;

nemzetközi szervezet: a nemzetközi közjog hatálya alá tartozó szervezet vagy annak alárendelt szervei, vagy olyan egyéb szerv, amelyet két vagy több ország közötti megállapodás hozott létre vagy amely ilyen megállapodás alapján jött létre;

nyilvánosságra hozatal: az adat bárki számára történő hozzáférhetővé tétele;

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 helyzetéhez, egészségi állapothoz, személyes preferenciákhoz, érdeklődéshez, megbízhatóságához, viselkedéshez, tartózkodási helyhez vagy mozgáshoz kapcsolódó jellemzők elemzésére vagy előrejelzésére használják;

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

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.