



Teresztenye Község Önkormányzata

3757 Teresztenye, Rákóczi Ferenc út 18

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:

2023.09.01.

jóváhagyta:


.....
Brogli Attila

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.....	14
1.10. Adatvédelmi tisztviselő.....	14
1.11. Képzés.....	14
1.12. Az adatvédelmi audit.....	15
1.13. A szervezeti egységek működtetéséhez kapcsolódó általános adatvédelmi szabályok	16
2. A szervezet adatvédelmi feladatai	17
2.1. Adatvédelmi tisztviselő kijelölése	17
2.2. Adatkezelési, adatfeldolgozói tevékenységek nyilvántartása	19
2.3. Átlátható tájékoztatás, kommunikáció és az érintett jogainak gyakorlására vonatkozó intézkedések.....	20
2.3.1. Tájékoztatás és a személyes adatokhoz való hozzáférés joga.....	20
2.3.2. Az érintett hozzáférési joga.....	22
2.3.3. Az érintett helyesbítéshez való joga	23
2.3.4. A törléshez, elfeledtetéshez való jog	23
2.3.5. Az adatkezelés korlátozásához való jog	24
2.3.6. A személyes adatok helyesbítéséhez vagy törléséhez, illetve az adatkezelés korlátozásához kapcsolódó értesítési kötelezettség	24
2.3.7. Az adathordozhatósághoz való jog.....	24
2.3.8. A tiltakozáshoz való jog	24
2.3.9. Automatizált döntéshozatal egyedi ügyekben, profilalkotás.....	25
2.3.10. A személyes adatokkal összefüggő jogok érvényesítése az érintett halálát követően.....	25
2.4. Az érintetti kérelmek kezelése	26
2.5. Az adatkezelés biztonsága, technikai és szervezési intézkedések végrehajtása	29
2.6. Az adatvédelmi incidensek.....	29
2.6.1. Incidensek belső nyilvántartása.....	29
2.6.2. Incidens NAIH bejelentése	30
2.6.3. Érintettek tájékoztatása az incidensről	30
2.6.4. Adatvédelmi incidensek kezelése	31
2.7. Érdekmérlegelés	32
2.8. Adatközlés, adattovábbítás, nyilvánosságra hozatal.....	33
2.8.1. Adattovábbítás harmadik országokba	33
2.9. Adatfeldolgozás, adatfeldolgozói garancianyújtás.....	34
2.10. Kötelező adatkezelések felülvizsgálata.....	36
2.11. Adatvédelmi hatásvizsgálat.....	37
3. Személyes adatok kezelése, nyilvántartása.....	38

3.1.	Munkavállalók adatkezelései	38
3.2.	Ügyfelekkel, szakfeladatokkal kapcsolatos adatkezelések	42
3.2.1.	Okmánymásolás	43
4.	Technikai és szervezési intézkedések	44
4.1.	Adminisztratív védelmi intézkedések.....	44
4.2.	Fizikai védelmi intézkedések	47
4.3.	Logikai védelmi intézkedések	48
4.4.	Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény hatálya alá tartozó szervek további követelményei	51
	Fogalomtár	53
	Mellékletek	56
1.	számú melléklet – Hozzáférés iránti kérelem (minta)	57
2.	számú melléklet – Helyesbítés iránti kérelem (minta).....	58
3.	számú melléklet – Törlés iránti kérelem (minta).....	59
4.	számú melléklet – Adatkezelés korlátozása iránti kérelem (minta).....	60
5.	számú melléklet – Tiltakozásra vonatkozó nyilatkozat (minta).....	61
6.	számú melléklet – Érintetti tájékoztatás adatvédelmi incidensről (minta)	62
7.	számú melléklet – Bemutatott okmányról készült feljegyzés (minta).....	63
8.	számú melléklet – Nyilatkozat a bemutatott hatósági okmányokról (minta)	64
9.	számú melléklet – Feljegyzés szóban előterjesztett érintetti kérelemről (minta)	65
10.	számú melléklet – Felhívás személyazonosság megerősítéséhez szükséges információk nyújtására	66
11.	számú melléklet – Érintetti kérelem elutasítása (minta)	68
12.	számú melléklet – Munkavállalói nyilatkozat számítástechnikai eszköz használatáról (minta)	69

Verzió: v1.03

Vezetői nyilatkozat

A Teresztenye Község 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 Teresztenye Község 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.

2023.09.01.

.....
Brogli Attila

Adatkezelő/adatfeldolgozó adatai

Adatkezelő, adatfeldolgozó neve: Teresztenye Község Önkormányzata

Címe (hivatalos levelezési cím): 3757 Teresztenye, Rákóczi Ferenc út 18

E-mail cím: teresztenyefonix@gmail.com

Telefonszáma: +36 48 463502

Honlapjának elérhetősége:

Adószáma: 15547633-1-05

Képviselője neve: Brogli Attila

Adatkezelési tájékoztató elérhetősége: 3757 Teresztenye, Rákóczi Ferenc út 18

Adatvédelmi tisztviselő neve: GDPRReg Kft.

Adatvédelmi tisztviselő elérhetősége: adatvedelem@teresztenye.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 tartsák, 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 Teresztenye Község 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.

Az Infotv. hatálya alá tartozó adatkezelések esetében jelen szabályzat rendelkezései akkor és annyiban alkalmazandóak, ha és amennyiben az adatkezelésre vonatkozó különös szabályzat (például Közterületi térfigyelő kamerarendszer adatvédelmi szabályzat) rendelkezései nem ellentétesek jelen szabályzat rendelkezéseivel, továbbá a különös szabályzatban nem szabályozott kérdések esetében.

Jelen 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
- 1999. évi LXIII. törvény a közterület-felügyeletről (Kftfv.)
- 2011. évi CLXV. törvény a polgárőrségről és a polgárőri tevékenység szabályairól (Pötv.)
- 1994. évi XXXIV. törvény a Rendőrségről (Rtv.)
- 2012. évi I. törvény a munka törvénykönyvéről (Mt.)
- 2011. évi CXCV. törvény a közszolgálati tisztviselőkről (Kttv.)
- 1992. évi XXXIII. törvény a közalkalmazottak jogállásáról (Kjt.)
- 2013. évi V. törvény a polgári törvénykönyvről (Ptk.)
- 2011. évi CXCV. törvény az államháztartásról (Áht.)

- 2011. évi CLXXXIX. törvény Magyarország helyi önkormányzatairól (Mötv.)
- 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 (Kp.)
- 1995. évi CXVII. törvény a személyi jövedelemadóról (Szja.)
- 2017. évi CL. törvény az adózás rendjéről (Art.)
- 1997. évi LXXXI. törvény a társadalombiztosítási nyugellátásról (Tny.)
- 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>
- Európai Adatvédelmi Testület iránymutatásai: <https://naih.hu/edpb-iranymutatasai>
- **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)
 - Közterületi térfigyelő kamerarendszer adatvédelmi szabályzat
 - Iratkezelési szabályzat

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 megállapításához, 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 orvostechnikai 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 tényt, 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. Ennek alapján, ha az érintett hozzájárulását olyan írásbeli nyilatkozat keretében adja meg, amely más ügyekre is vonatkozik, a hozzájárulás iránti kérelmet ezektől a más ügyektől egyértelműen megkülönböztethető módon kell előadni, érthető és könnyen hozzáférhető formában, világos és egyszerű nyelvezettel. Az érintett hozzájárulását tartalmazó ilyen nyilatkozat bármely olyan része, amely sérti a Rendeletet, kötelező erővel nem bír. A hozzájárulás egy adatkezelési cél érdekében végzett adatkezeléshez való hozzájárulást jelenti. Ha az adatkezelés egyszerre több célt is szolgál, akkor a hozzájárulást az összes adatkezelési célra vonatkozóan meg kell adni. 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 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.

Kizárólag akkor képezheti a Szervezet adatkezelésének jogalapját az érintetti hozzájárulás, ha az adatkezelés vonatkozásában igazolható módon nincs az érintett és a Szervezet között egyértelműen egyenlőtlen viszony, továbbá szervezési és technikai intézkedésekkel biztosítható, hogy az érintett hozzájárulását bármikor ugyanolyan könnyen visszavonhassa, ahogy azt megadta.

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

A Teresztenye Község 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. **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 hozzáférés joga:** 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 fenn, más jogalapok fennállta, így többek között a jogi kötelezettség teljesítése alapján kezelt adatok esetén pedig kifejezetten korlátozott ez a joga, illetve nem áll fenn.
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. A 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 Teresztenye Község 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, továbbá felelős azért, hogy a Szervezet tevékenysége során betartsa jelen Adatvédelmi és adatbiztonsági szabályzatban foglalt követelményeket. 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 Szervezet vezetőjének a felelőssége, hogy gondoskodik a foglalkoztatottak megfelelő adatvédelmi tudatosságáról. Ennek megfelelően a vezető gondoskodik a szükséges felkészültségről, kompetenciáról

valamennyi foglalkoztatott esetében, akik 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 részt vevő 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 szerepükkel és annak fontosságával.

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 foglalkoztatottak 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.

1.12. Az adatvédelmi audit

Az adatkezelő felelőssége, hogy meghatározott rendszerességgel, súlyos probléma felmerülése esetén soron kívül, vagy az adatvédelmi tisztviselő javaslatára soron kívüli vizsgálatot folytasson le annak érdekében, hogy a Szervezet eljárása maradéktalanul megfeleljen az adatvédelmi és adatbiztonsági előírásoknak (adatvédelmi audit).

Az adatkezelő az adatvédelmi audit végrehajtására tervet készít.

Az adatvédelmi audit célja, hogy megvizsgálja a Szervezet adott rendszere, eljárása mennyire felel meg a Rendeletnek és a hatályos adatvédelmi előírásoknak, felügyeleti hatósági elvárásoknak.

A Szervezet vezetőjének a felelőssége, hogy kijelölje az adatvédelmi audit lefolytatásában közreműködőket. Az adatvédelmi auditot az adatvédelem területén szakértelemmel/gyakorlattal rendelkező, legalább három tagból álló bizottság látja el. Az Adatvédelmi tisztviselő minden esetben részt vesz az auditálásban. A Szervezet jogosult külső adatvédelmi szakértő segítségét igénybe venni az adatvédelmi audit lefolytatásában.

Az adatvédelmi audit során az auditáló bizottság különösen az alábbiak megfelelőségét vizsgálja:

- alapelvek érvényesülését,
- személyes adatkezelések azonosítási gyakorlatát a kijelölt szervezeti egységnél,
- adatkezelések és adatfeldolgozások nyilvántartását,
- adatkezelési tájékoztatókat,
- érdekmérlegelési tesztek helyzetét,
- érintetti jogok gyakorlásához szükséges eljárásokat,
- hatásvizsgálatok állapotát,
- incidenskezelés és nyilvántartás gyakorlatát,
- adatbiztonsági eljárásokat,
- személyes adatok harmadik országokba vagy nemzetközi szervezetek részére történő továbbítását,

- dokumentált szabályzatokat, egyéb belső szabályozókat,
- adatvédelmi tudatosság növelésének és dokumentálásának gyakorlatát.

Az auditált szervezeti egységek kötelesek az auditáló bizottsággal együttműködni, a megfelelő tájékoztatásokat, felvilágosításokat megadni. A szervezeti egységek vezetői felelnek azért, hogy a foglalkoztatottak, az adatkezelésre rálátással rendelkező személyek a bizottság által feltett kérdésekre a legjobb tudásuk szerint válaszoljanak, valamint a szervezeti egységek vezetői maguk is kötelesek a vizsgálatban proaktívan részt venni, a hozzájuk intézett kérdésekre maradéktalanul választ adni.

Az adatvédelmi audit kockázatelemzésen alapul, melynek során az auditáló bizottság azt vizsgálja, hogy a Szervezet adatkezeléssel kapcsolatos tevékenységének nem megfelelése milyen hatással lehet az érintettekre.

Az adatvédelmi audit eredményeként az auditáló bizottság adatvédelmi jelentést készít, mely tartalmazza az adatvédelmi kockázatokkal kapcsolatos megállapításokat és a Szervezet adatvédelmi (jog)szabályi megfelelésének biztosítására vonatkozó konkrét javaslatokat. Az adatvédelmi jelentést a Szervezet vezetője hagyja jóvá és gondoskodik az abban foglaltak végrehajtásáról.

1.13. A szervezeti egységek működtetéséhez kapcsolódó általános adatvédelmi szabályok

A Szervezet vezetője határozza meg a szervezettel munkaviszonyban, illetőleg munkavégzésre irányuló jogviszonyban álló személyek adatkezeléssel kapcsolatos feladatait, mely feladatok arra irányulnak, hogy törvényes és tisztességes módon, az adatkezelés minden szakaszában biztosítsák az adatok pontosságát, gondoskodjanak az érintett személyes adatainak védelméről.

Jogszámban meghatározott kötelezettség teljesítése miatt, vagy a Szervezet döntése alapján szükséges új adatkezelés bevezetéséről, vagy folyamatban lévő adatkezelés módosításáról a Szervezet vezetője dönt.

A Szervezet vezetője a szervezeti egységek vezetőjét jelöli ki, hogy vegyenek részt a Szervezet adatvédelmi megfelelésének elősegítésében, továbbá kísérik figyelemmel a szervezeti egységeknél folytatott adatkezeléseket.

Az adatkezelésért felelős szervezeti egység vezetőjét és az Adatvédelmi tisztviselőt az új adatkezelés bevezetésére, vagy folyamatban lévő adatkezelés módosítására vonatkozó igény megfogalmazásától kezdve be kell vonni az adatkezelés feltételeinek kidolgozása folyamatába.

Amennyiben az új adatkezelés bevezetése, vagy folyamatban lévő adatkezelés módosítása több szervezeti egységet érint, az adatkezelésért felelős valamennyi érintett szervezeti egység vezetőjét és az Adatvédelmi tisztviselőt be kell vonni az adatkezelés feltételeinek kidolgozása folyamatába.

Az adatkezelés feltételeinek kidolgozásában érintett szervezeti egységek vezetői kötelesek egymással és az Adatvédelmi tisztviselővel együttműködni. Az adatkezelés feltételeinek kidolgozásában érintett szervezeti egységek tevékenységének koordinálásáról és az Adatvédelmi tisztviselővel való együttműködés megteremtésének feltételeiről a Szervezet vezetője gondoskodik.

Az adatkezelés bevezetésével, módosításával az adatkezelés feltételeinek meghatározásával kapcsolatban az adatkezelésért annak tárgya szerint felelős szervezeti egység vezetője (több érintett szervezeti egység vezetője egymással együttműködve):

- meghatározza az adatkezelés célját, az adatkezelés jogalapját, a kezelendő adatok körét, az adatkezelés egyéb feltételeit, és ilyen tartalmú javaslatot készít a döntésre jogosultnak,

- adott esetben elemzi, hogy az eltérő célú adatkezelés összeegyeztethető-e az adatkezelés eredeti céljával, amelyekre a személyes adatokat gyűjtötték,
- amennyiben az adatkezeléshez szükséges, elkészíti az érdekmérlegelési teszt dokumentumának tervezetét,
- az Adatvédelmi tisztviselő véleményének kikérése után dokumentálja az adatvédelmi hatásvizsgálat el nem végzésének indokait vagy javaslatot tesz a döntésre jogosultnak adatvédelmi hatásvizsgálat elvégzésére; (Pozitív döntés esetén az adatvédelmi hatásvizsgálatot lefolytató munkacsoport felállításáról a Szervezet vezetője határoz, mely munkacsoportba a tervezett adatkezeléssel érintett szervezeti egységek kötelesek résztvevőt delegálni.),
- előterjesztést tesz a döntésre jogosultnak arról, hogy az adatkezelés közös adatkezelésként indokolt-e ellátni, valamint szükséges-e adatfeldolgozót igénybe venni,
- az adatkezelés bevezetéséről, illetve az adatkezelés módosításáról szóló döntést követően közreműködik az új adatkezelés GDPR Reg Adatkezelési rendszerben történő rögzítésében.

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 közvetlenül az Adatvédelmi tisztviselőhöz is fordulhatnak; ebben az esetben az Adatvédelmi tisztviselő köteles az érintetti kérelmet haladéktalanul a Szervezet vezetője vagy – ha van – a kijelölt felelős részére továbbítani,
- a Szervezet foglalkoztatottja a személyes adatok kezelésével kapcsolatos valamennyi kérdésben és a Rendelet értelmezésével kapcsolatban közvetlenül jogosult az Adatvédelmi tisztviselőhöz fordulni,
- 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,
- együttműködik az adatkezeléssel érintett szervezeti egységek vezetőivel egy új adatkezelés tervezett bevezetése esetén,
- kérésre szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, valamint nyomon követi a hatásvizsgálat elvégzését,
- közreműködik az adatvédelmi incidens kezelésében, kivizsgálásában,
- közreműködik az adatvédelmi audit lefolytatásában,
- közreműködik a belső adatvédelmi és adatbiztonsági szabályzat megalkotásában, módosításában,
- 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 jogosult:

- tájékoztatást, felvilágosítást kérni a Szervezet valamennyi adatkezelési tevékenységéről,
- a Szervezet valamennyi adatkezelését vizsgálni és minden olyan helyiségbe belépni, ahol adatkezelés folyik;
- tanácskozási és véleményezési joggal részt venni minden olyan fórumon, ahol a feladatai ellátásával összefüggő kérdések szerepelnek a napirenden,
- javaslatot tenni közvetlenül a Szervezet vezetőjének valamely személyes adatok kezelését érintő kérdésben,
- felszólítani az adatkezelésben részt vevő személyt a jogszerű állapot helyreállítására,
- kezdeményezni a Szervezet adatvédelmi előírásainak, valamint a kialakult adatkezelési gyakorlat átalakítását, vagy az adatkezelést érintő más szükséges intézkedések megtételét.

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 Szervezet vezetője gondoskodik az Adatvédelmi tisztviselő kijelöléséről, melynek tényéről, továbbá az Adatvédelmi tisztviselő személyéről és közvetlen elérhetőségeiről a Szervezet foglalkoztatottjait írásban tájékoztatja.

A Teresztenye Község 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 Teresztenye Község 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 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 Teresztenye Község 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 a 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 jogszabályon vagy szerződéses kötelezettségen alapul vagy szerződés kötésének előfeltétele-e, valamint hogy az érintett köteles-e a személyes adatokat megadni, továbbá hogy milyen lehetséges következményeikkel járhat az adatszolgáltatás elmaradása,
- 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 a fentiekén kívül rendelkezésre kell 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 Teresztenye Község 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 akár egyedileg létrehozott kategóriával kapcsolatos adatkezelési tájékoztatók).

Az Ügyfelekkel kapcsolatos aktuális adatkezelési tájékoztató honlapon is publikálásra kerül, 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 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 címzettekéről 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 közvetlenül gyermekeknek kínált, 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,
- 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,
- jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez.

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 közérdekéből 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 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, személyazonosítása mellett lehetősége van bármely általa választott, személyesen, postai úton, elektronikus levélben, meghatalmazott útján, illetve egyéb módon kérelmet benyújtani. Az érintetti kérelemnek kötelező tartalmi elemei nincsenek, formanyomtatványhoz nem kötött. Az érintettek jogainak gyakorlását elősegítve, jelen szabályzat 1-5. mellékletei szerinti minták szabadon használhatók, de nem kötelezők.

A tájékoztatást az érintett által kért módon, elektronikus úton benyújtott kérelem esetén lehetőség szerint elektronikus úton kell megadni.

A Teresztenye Község Önkormányzata megfelelő intézkedéseket hoz 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.

Adatkezelő 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 adatkezelő 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. Amennyiben az érintett közvetlenül az Adatvédelmi tisztviselőhöz fordult panaszával, az Adatvédelmi tisztviselő köteles a panaszt továbbítani a Szervezet vezetőjének.

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. Valamely okiratról készült egyszerű elektronikus másolat, vagy nem hitelesített nem elektronikus másolat megküldése a személy azonosítására nem alkalmas, ezért e célra azok megküldését a kérelmet előterjesztő személytől kétség felmerülése esetén sem lehet kérni.

Érintetti kérelem csak abban az esetben teljesíthető, ha az adatkezelő minden kétséget kizáróan megállapította a kérelmező személyazonosságát. Amennyiben megalapozott kétség merül fel a kérelmező személyazonosságában, az érintetti kérelemben foglaltak semmilyen módon nem teljesíthetők. Adatkezelő kiegészítő információt kérhet a kérelmező személy személyazonosságának értékelése céljából, azonban ez nem vezethet túlzó kérésekhez és olyan személyes adatok begyűjtéséhez, amelyek nem relevánsak vagy szükségesek az egyén és a kért személyes adat közötti kapcsolat megerősítése szempontjából.

Eljárásrend a kérelmező személyazonosságának megállapítása érdekében:

A. Érintetti kérelem személyes benyújtása:

Amennyiben az érintett vagy képviselője személyesen kívánja gyakorolni az GDPR 15-21. cikk szerinti jogait, adatkezelő nevében eljáró ügyintéző köteles az érintett személyazonosságát minden kétséget kizáró módon megállapítani. Kérelmező a személyazonossága megállapításához az ügyintéző felhívására köteles a személyazonosító okmányát bemutatni. A személyazonosító okmány bemutatásáról feljegyzést (7. sz. melléklet) kell készíteni vagy a kérelmezőt nyilatkoztatni (8. sz. melléklet) szükséges. Az érintett nevében eljáró törvényes vagy meghatalmazott képviselő esetén a képviselői jogot okirattal igazolni szükséges.

Az érintetti kérelemről az ügyintéző feljegyzést készít, amennyiben a kérelmező szóban kívánja előadni az érintetti kérelmét. Az érintetti kérelemről szóló feljegyzés minimális tartalmi elemeit a 9. sz. melléklet tartalmazza. Amennyiben a személyesen megjelent kérelmező papír alapon terjeszti elő a kérelmét, az ügyintéző a papír alapú érintetti kérelmet iktatja.

B. Érintetti kérelem telefonon történő előterjesztése:

Adatbiztonsági okok miatt az érintetti kérelmek telefonon történő előterjesztésére csak szűk körben van lehetőség. Telefonon előterjesztett kérelem esetén, a kérelmező teljes nevén és telefonszámán kívül az ügyintéző köteles legalább három olyan személyazonosító és egyéb személyes adat bemondását kérni kérelmezőtől, amely lehetővé teszi az egyértelmű azonosítást. Ilyen adatnak minősülhet a kérelmező születési neve, születési helye és ideje, anyja neve, lakcíme, amennyiben ezen adatokat adatkezelő nyilvántartása is tartalmazza. A megismert adatokról és az érintetti kérelem tartalmáról az ügyintéző feljegyzést (9. sz. melléklet) készít. A telefonon előterjesztett kérelemre azonnali tájékoztatás csak abban az esetben adható, és intézkedés csak abban az esetben tehető, ha a kérelmező minden kétséget kizáró módon az érintett és az

érintetti kérelem elérhetőségi adatok (e-mail cím, telefonszám) helyesbítésére vagy kiegészítésére irányul. Egyéb esetben az érintetti kérelem elbírálása és az érintett tájékoztatása írásban történik.

C. Érintetti kérelem elektronikus úton, e-mailben történő benyújtása:

Amennyiben az érintett elektronikus úton, e-mailben kívánja gyakorolni a GDPR 15-21. cikk szerinti jogait, adatkezelő köteles az érintett személyazonosságát minden kétséget kizáró módon megállapítani. Kérelmező személyazonosságának megállapítása érdekében adatkezelő elsősorban a kérelmező e-mail címét és a kérelemben megadott személyazonosító és egyéb személyes adatait veti össze a nyilvántartásában szereplő adatokkal. Amennyiben a kérelmező személyazonossága egyértelműen megállapítható, a kérelemben foglaltakra intézkedni szükséges. Amennyiben a kérelmező személyazonossága minden kétséget kizáró módon nem állapítható meg, a kérelmező további, a személyazonosságának megerősítéséhez szükséges információk nyújtására kérhető. Annak eldöntésére, hogy milyen további információk és milyen módon kerüljenek benyújtásra, az eset összes körülményét mérlegelve kell eldönteni és indokolni szükséges. Amennyiben az adatok biztonsága másként nem garantálható, adatkezelő jogosult teljes bizonyító erejű magánokirat vagy közokirat benyújtását kérni kérelmezőtől.

D. Érintetti kérelem postai úton történő benyújtása:

Amennyiben az érintett postai úton megküldött kérelmével kívánja gyakorolni a GDPR 15-21. cikk szerinti jogait, adatkezelő köteles az érintett személyazonosságát minden kétséget kizáró módon megállapítani. Kérelmező személyazonosságának megállapítása érdekében adatkezelő elsősorban a kérelmező postai címe és a kérelemben megadott személyazonosító és egyéb személyes adatait veti össze a nyilvántartásában szereplő adatokkal. Amennyiben a kérelmező személyazonossága egyértelműen megállapítható, a kérelemben foglaltakra intézkedni szükséges. Amennyiben a kérelmező személyazonossága minden kétséget kizáró módon nem állapítható meg, a kérelmező további, a személyazonosságának megerősítéséhez szükséges információk nyújtására kérhető. Annak eldöntésére, hogy milyen további információk és milyen módon kerüljenek benyújtásra, az eset összes körülményét mérlegelve kell eldönteni és indokolni szükséges. Amennyiben az adatok biztonsága másként nem garantálható, adatkezelő jogosult teljes bizonyító erejű magánokirat vagy közokirat benyújtását kérni kérelmezőtől.

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, illetve 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 rendelkezés hiányában a kérelem teljesítéséért megállapítható költségek a 301/2016. (IX. 30.) Korm. rendeletben foglalt költségek figyelembevételével kerülnek megállításra.

A Teresztenye Község Önkormányzata az érintettek kérelmeit a GDPR Reg Adatkezelési rendszerben is nyilvántarthatja, elkészítheti a szükséges dokumentumokat. A rendszer támogatja az adatkezelőt az érintett magánszemélyek GDPR 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 jogorvoslathoz való jogról.

2.5. Az adatkezelés biztonsága, technikai és szervezési intézkedések végrehajtása

A Teresztenye Község 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 költsönhatását, 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 Teresztenye Község 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 Teresztenye Község Önkormányzata mint adatkezelő kötelessége, hogy amint tudomására jut egy adatvédelmi incidens (pl. felmerül a gyanú, hogy a Szervezet számítógépes biztonsági incidens áldozatává vált, vagy éppen ennek folyamata alatt van) azt indokolatlan késedelem nélkül vizsgálja, 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 tudomásszerzést követően indokolatlan késedelem nélkül bejelenti az adatkezelőnek.

2.6.1. Incidensek belső nyilvántartása

A Szervezet nyilvántartja az adatvédelmi incidenseket, feltüntetve az adatvédelmi incidenshez kapcsolódó tényeket, annak hatásait és az orvoslására tett intézkedéseket annak érdekében, hogy a felügyeleti hatóság ellenőrizhesse a GDPR vonatkozó követelményeinek való megfelelést.

Az adatvédelmi incidensek belső nyilvántartása legalább az alábbi adatokat tartalmazza:

- az adatvédelmi incidensről készült ügyirat iktatószámát,

- az adatvédelmi incidens rövid leírását, beleértve az érintett irat vagy nyilvántartás, elektronikus információs rendszer megjelölését vagy azonosítóját,
- az incidensről való tudomásszerzés időpontját és az incidens bekövetkezésének megállapított vagy valószínűsített időpontját,
- az incidenssel érintett személyes adatok kategóriáját,
- az incidens hatásait, következményeit, valamint az orvoslásukra tett intézkedéseket,
- a bejelentés időpontját, vagy a mellőzés okát.

Amennyiben az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve, akkor a bejelentést mellőzve, a Szervezet az incidenst kizárólag az adatvédelmi incidensek belső nyilvántartásába veszi. Ilyen esetben a nyilvántartás tartalmazza a mellőzés rövid indokolását.

2.6.2. Incidens NAIH bejelentése

A Szervezet 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 bejelentésnek 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 megtehessék 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 az észlelő személy késedelem nélkül, a megadott kapcsolattartási csatornák valamelyikén értesíti a szervezeti egysége vezetőjét és a Szervezet vezetője általa kijelölt felelőst vagy az Adatvédelmi tisztviselőt vagy hiányában a kapcsolattartásra kijelölt felelőst.

Az adatvédelmi incidenst észlelő személy köteles a tapasztalt jelenséget minden rendelkezésére álló eszközzel dokumentálni, azokat haladéktalanul a Szervezet vezetője által kijelölt felelős vagy az Adatvédelmi tisztviselő, vagy ha ez nem lehetséges, a szervezeti egység vezetője 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; amennyiben az adatvédelmi incidens a Szervezet által igénybe vett adatfeldolgozó tevékenységével kapcsolatban következett be, az adatvédelmi incidens körülményeinek, és az azzal összefüggő lehetséges kockázatok és hatások kivizsgálásába az adatfeldolgozó képviselőjét is be kell vonni,
- értesíti a Szervezet vezetőjét és – ha korábban nem történt meg - az Adatvédelmi tisztviselőt,
- 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 rendszer 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 adatvédelmi incidenst a Nemzeti Adatvédelmi és Információszabadság Hatóságnak, kivéve, ha az 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 az illetékes hatósággal, akkor azokat további indokolatlan késedelem nélkül később részletekben közli,
- 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, továbbképzésének.

A Teresztenye Község Önkormányzata az adatvédelmi incidensek nyilvántartására és 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. Érdelmérlegelés

Az 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. 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.

A jogos érdekre hivatkozást mint jogalapot nem lehet alkalmazni a közhatalmi szervek által feladataik ellátása során végzett adatkezelésre. Közhatalmi szervek esetén a jogalkotó feladata, hogy jogszabályban határozza meg a kötelező adatkezelések részleteit. Ebben az esetben a közhatalmi szerv adatkezelése a Rendelet 6. cikk (1) bekezdés c) pontja jogalapon történik, vagyis az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges, vagy az e) pont szerinti jogalapon alapul, amikor az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges. Ha az adatkezelés jogi kötelezettség teljesítéséhez szükséges, akkor nincs szükség arra, hogy az adatkezelő mérlegelje akár a saját, akár harmadik fél jogos érdekeit. Ha a közfeladatot előíró vagy a közhatalmi feladatot megállapító jogszabályok nem tartalmazzák az Infotv. 5. § (3) bekezdése szerinti adatkezelési körülményeket, az adatkezelő az általános adatvédelmi szabályok, különösen a személyes adatok kezelésére vonatkozó elvek szerint jogosult, meghatározott esetekben köteles adatkezelési tevékenységet végezni, és annak jogszerűségét az elszámoltathatóság elvének megfelelően igazolni.

A Szervezet a jogos érdek jogalapon kívüli, más jogalapon történő adatkezelés mellett is elvégezheti az érdelmérlegelési tesztet az érintett magánszférájának arányos korlátozása, valamint az elszámoltathatóság igazolása érdekében.

Az érdelmérlegelés 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. Az adatkezelés akkor lehet jogszerű, ha az érdekmérlegelési teszt eredménye az, hogy az adatkezelés szükséges és arányos, adatkezelő jogos érdeke megállapítható.

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 ésszerűen 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.

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.

A Szervezet 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 adat csak akkor hozható nyilvánosságra, ha a Szervezet erre megfelelő joggal 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 Vezető felelős 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, adatfeldolgozóknak 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 – a Rendelet és jelen szabályzat rendelkezései is figyelemmel – teljesíti a harmadik országok vagy nemzetközi

szervezeteknek történő adattovábbításra vonatkozó, a Rendeletben és jelen szabályzatban 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 az elektronikus információs rendszerek biztonságának felügyeletét ellátó 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 közös adatkezelő:

Amennyiben a Szervezet vezetőjének döntése alapján a Szervezet meghatározott feladatának érdekében közös adatkezelői jogviszony létesítése indokolt, a közös adatkezelők átlátható módon, a közöttük létrejött megállapodásban határozzák meg a Rendelet szerinti kötelezettségeik teljesítéséért fennálló, különösen az érintett jogainak gyakorlásával és az érintett tájékoztatásával kapcsolatos információk rendelkezésre bocsátásából eredő feladataikkal összefüggő felelősségük megoszlását, kivéve azt az esetet és annyiban, ha és amennyiben az adatkezelőkre vonatkozó felelősség megoszlását a rájuk alkalmazandó uniós vagy tagállami jog határozza meg. A megállapodásban az érintettek számára kapcsolattartót lehet kijelölni.

A közös adatkezelői megállapodásnak megfelelően tükröznie kell a közös adatkezelők érintettekkel szembeni szerepét és a velük való kapcsolatukat. A megállapodás lényegét az érintett rendelkezésére kell bocsátani.

Az érintett a közös adatkezelői megállapodás feltételeitől függetlenül mindegyik adatkezelő vonatkozásában és mindegyik adatkezelővel szemben gyakorolhatja a Rendelet szerinti jogait.

A közös adatkezelői megállapodás tartalmának összeállítása során ki kell kérni az Adatvédelmi tisztviselő véleményét.

A Szervezet mint adatfeldolgozó:

A Teresztenye Község 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.

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 a kötelező adatkezelések (Rendelet 6. cikk (1) bek. c) és e) pontok) 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 Teresztenye Község Önkormányzata a GDPR Reg Adatkezelési rendszerben végzi el és dokumentálja az adatkezelések felülvizsgálatát az egyes adatkezelésekre beállított felülvizsgálati gyakorisággal.

2.11. Adatvédelmi hatásvizsgálat

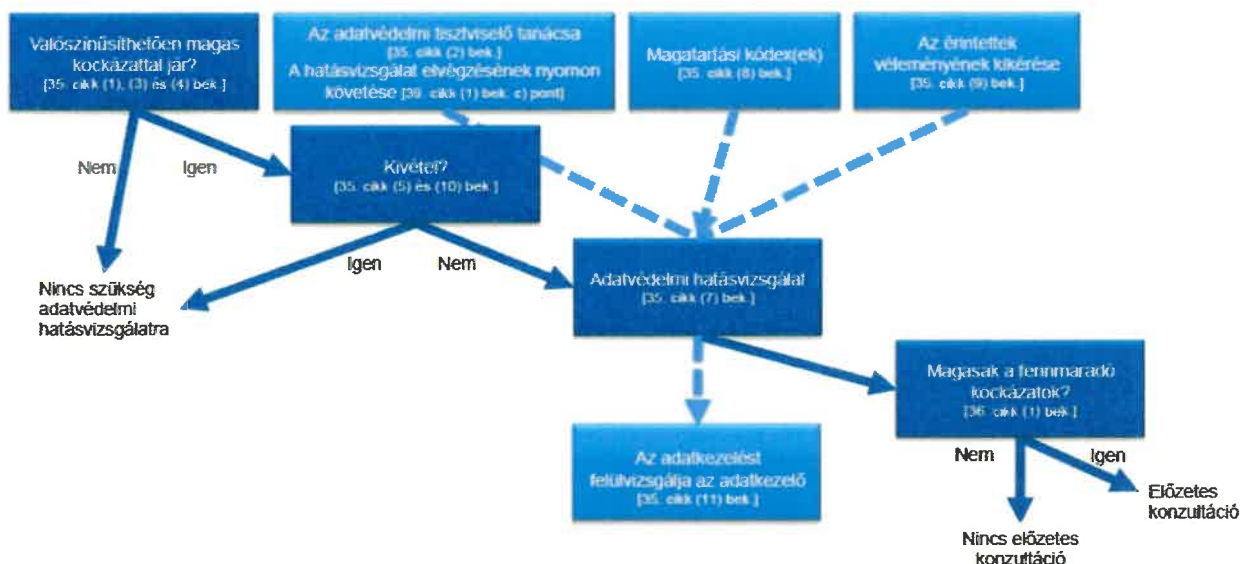
A természetes személyek jogaira és szabadságaira nézve magas kockázattal járó esetekben az adatkezelő – annak érdekében, hogy az adatkezelés jellegét, hatókörét, körülményeit és céljait, valamint a kockázat forrásait figyelembe véve felmérje a magas kockázat különös valószínűségét és súlyosságát – az 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 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 felelősökből álló, az adatvédelmi hatásvizsgálat lefolytató munkacsoport végzi el, szükség szerint be kell vonni az érintett vezetőket, felelősöket (pl. informatikai, informatikai biztonsággal foglalkozó felelősöket). Az adatvédelmi hatásvizsgálatot lefolytató munkacsoportba a tervezett adatkezeléssel érintett szervezeti egységek kötelesek résztvevőt kijelölni. Az Adatvédelmi tisztviselő szakmai tanácsát ki kell kérni, a döntés során figyelembe kell venni.

Az Európai Adatvédelmi Testület által elfogadott – vagy a GDPR alkalmazandóvá válását követően fenntartott –, az adatvédelmi hatásvizsgálatra vonatkozó hatályos iránymutatásban foglalt szempontokat és eljárásrendet a munkacsoport köteles figyelembe venni.

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, vagy a hatásvizsgálat mellőzésének okait dokumentálni kell, a vizsgálat során figyelembe kell venni a felügyeleti hatóság által összeállított adatkezelések jegyzékét.

A Teresztenye Község 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 alapján.

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 Teresztenye Község 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 Teresztenye Község 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 fenn 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 válasza 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 Teresztenye Község 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.

Figyelemmel arra, hogy adatkezelő közhatalmi jogosítványt gyakorló szerv, a munkavállalókkal (beleértve valamennyi munkavégzésre irányuló jogviszonyban álló foglalkoztatottat) kapcsolatos, jelen fejezet hatálya alá tartozó adatkezeléseket a GDPR 6. cikk (1) bekezdés e) pontja (közhatalmi jogosítvány jogalap) alapján kezeli. A jelen Adatvédelmi és adatbiztonsági szabályzat 2.7. pontjában foglaltakra tekintettel, amennyiben szükséges, munkáltató az adatkezeléséhez fűződő jogos érdek fennállásának megállapításához érdemlélegelést 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 Teresztenye Község Önkormányzata az adatkezeléshez fűződő jogos érdeke fennállásának megállapításához szükséges érdekmérlegelést a GDPR Reg Adatkezelési rendszerben dokumentálja. Az Érdekmérlegelés – 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 magánhasználata.

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.

A munkáltató a fokozatosság elvét betartva, lépcsőzetes rendszert vezet be a számítástechnikai eszközök (pl. laptop, számítógép, telefon), e-mail fiókok és az internet jogszerű használatának ellenőrzése céljából.

Munkáltató a tervezett munkahelyi ellenőrzésről köteles kikérni az adatvédelmi tisztviselő véleményét. A munkáltató legalább az ellenőrzés tényéről, annak időpontjáról, az ellenőrzés céljáról, továbbá az ellenőrzést végző személyekről előzetesen írásban vagy elektronikus úton tájékoztatja az ellenőrzésben érintett szervezeti egységeket. A tájékoztatást olyan időben és módon kell megtenni, hogy az lehetővé tegye a jog gyakorlását és kötelezettség teljesítését. A szervezeti egység vezetőjének a kötelessége a szervezet valamennyi munkavállalóját megfelelően és haladéktalanul tájékoztatni az ellenőrzés tényéről, céljáról, időpontjáról és egyéb releváns információkról akként, hogy a tájékoztatás ténye és tartalma utólagosan megállapítható legyen. Munkáltató vélelmezi, hogy a munkahelyi infrastruktúrát munkavállaló jogszerűen használja, munkavállaló a számítástechnikai eszközön, rendszerben magáncélú személyes adatokat nem tárol. Munkavállaló a tiltás ellenére a munkahelyi infrastruktúrán tárolt, magáncélú személyes adatokat köteles legkésőbb az ellenőrzés megkezdése előtt törölni. Munkavállaló köteles az ellenőrzésen részt venni és az ellenőrzés során együttműködni, különösen az ellenőrzés során jelzéssel élni a munkáltató által jogszerűen nem kezelhető, vagyis meg nem ismerhető személyes adatok esetén. Munkavállaló jogosult az ellenőrzés eredményét megismerni és arra észrevételt tenni. A munkavállalói jelenlét hiánya nem lehet akadálya a munkáltatói ellenőrzés végrehajtásának; amennyiben a munkavállaló vagy meghatalmazottja az ellenőrzésen nem vesz részt, vagy meghatalmazás hiányában a szervezeti egység vezetője és az adatvédelmi tisztviselő jelenlétében, fokozott figyelemmel és az elszámoltathatóság elvére tekintettel, megfelelően dokumentáltan hajtható végre az ellenőrzés. Az e-mail fiók ellenőrzése során a munkáltató elsődlegesen az e-mail címet és

a levél tárgyát ismerheti meg, és ha ezen adatokból megállapítást nyer, hogy az e-mail magáncélú, az e-mail tartalma nem ismerhető meg. Abban az esetben, ha a munkáltató rendelkezésére áll azon információ, hogy vélelmezhetően e-mailben a munkáltató üzleti, gazdasági érdekeit sértő, védett információk, adatok kerültek harmadik félnek továbbításra, munkáltató a vélelmezett jogsértés időintervallumában kiküldött elektronikus levelek tartalmába betekinthez. A számítástechnikai eszközön tárolt dokumentumok, fájlok ellenőrzésére elsősorban a metaadatok szolgálnak. Az internethasználat ellenőrzése arra terjed ki, hogy a munkavállaló meg nem engedett honlapokat látogat-e munkaidőben. A munkáltató adat- és információbiztonsági megfontolásokból különösen tiltja a felnőtt tartalmú honlapok látogatását, továbbá azon honlapok látogatását, melyek nem köthetők a munkavégzéshez. A fokozatosság elvét betartva, a munkáltatói ellenőrzés során elsődlegesen a látogatott honlapok címe és a látogatás időpontja kerül megismerésre. Amennyiben feltételezhető, hogy a honlap látogatása a munkahelyi feladatokkal össze nem egyeztethető, vagyis magáncélú, a munkavállaló tevékenységének részletes feltérképezése főszabályként nem indokolt (vagyis azon tevékenységek, hogy a munkavállaló mit is csinált a honlapon, milyen felhasználó nevet és jelszót mentett el, esetleg milyen fájlokat mentett le a tiltott honlapról). A munkahelyi ellenőrzésről jegyzőkönyv készül, a jegyzőkönyvben legalább az ellenőrzés ténye és időpontja, az ellenőrzés eredménye, az esetleges jogsértés ténye és leírása szerepel akként, hogy a munkáltató által jogszerűen nem kezelhető személyes adatok jegyzőkönyvbe való felvételére nem kerülhet sor. A jegyzőkönyv tartalmazza az ellenőrzött munkavállaló ellenőrzés megállapításaira tett észrevételeit és az ellenőrzésen jelenlévők nevét, munkakörét és aláírását, valamint a jegyzőkönyv készítésének helyét és idejét.

Otthoni munkavégzés ellenőrzésére vonatkozó különös adatvédelmi szabályok

Amennyiben a munkavállaló kivételesen, ideiglenes jelleggel az állandó munkavégzési helytől eltérően a lakóhelyén végzi a munkát, a munkáltató az alábbi követelmények szerint jogosult ellenőrizni a munkavállaló otthoni munkavégzését:

- a munkáltatói ellenőrzés célja a munkavállalói kötelezettségek betartásának, a munkaidő és a jelenlét igazolása, különösen annak ellenőrzése, hogy a munkavállaló munkaidőben a munkáltató rendelkezésére áll és a rá bízott munkát személyesen, az általában elvárható szakértelemmel és gondossággal, a munkájára vonatkozó szabályok, előírások, utasítások és szokások szerint elvégzi;
- munkáltató az ellenőrzés tényéről, azok technikai és egyéb eszközeiről és feltételeiről előzetesen, írásban tájékoztatni köteles munkavállalót;
- az ellenőrzés csak munkaidőben történhet a munkaközi szünetre vonatkozó szabályok figyelembevételével;
- munkavállaló tevékenysége nem ellenőrizhető olyan szoftverrel, mely állandó megfigyelésére alkalmas, az ellenőrzés kizárólag időszakos lehet, és az nem jelenthet harmadik személy – így különösen a munkavállalóval egy háztartásban élő hozzátartozója – számára aránytalan terhet;
- munkáltató nem jogosult a munkavállalót a lakóhelyén ellenőrizni;
- munkakörtől függetlenül az ellenőrzés eszköze lehet például a munkavállaló napi jelentése az elvégzett feladatokról;
- munkáltató köteles az adatvédelmi tisztviselő véleményét kikérni az ellenőrzés részleteinek kidolgozásakor.

Munkáltatói ellenőrzés és az adatok archiválásának különös szabályai a munkaviszony megszűnésekor

Munkáltató a munkavállaló jogviszonyának megszűnése esetén, legkésőbb a munkáltató által biztosított számítástechnikai eszközök átadás-átvételekor munkahelyi ellenőrzést tart. Az ellenőrzés célja annak

megállapítása, hogy az eszköz rendeltetésszerű használatra alkalmas-e, a használt számítástechnikai eszköz új felhasználónak kiadható-e. Az ellenőrzést a munkáltató informatikus munkatársa végzi. A kilépő munkavállaló jogosult az ellenőrzésen részt venni, és részvétele esetén köteles jelzéssel élni a munkáltató által jogszerűen nem kezelhető, vagyis meg nem ismerhető személyes adatok esetén. A kilépő munkavállaló köteles a munkaviszonya megszűnése esetén, a munkáltató által biztosított számítástechnikai eszköz átadás-átvételét megelőzően a munkavégzéshez biztosított számítástechnikai eszközről törölni valamennyi, a számítástechnikai eszközön a tiltás ellenére tárolt magáncélú személyes adatot, beleértve különösen a magáncélú elektronikus levelezést, kép- és videófájlokat, dokumentumokat, internetes jelszavakat, keresési előzményeket. Munkavállaló e kötelezettség megszegése miatt a munkáltatónak okozott károkat köteles megtéríteni.

A kilépett munkavállaló számítástechnikai eszközeit a munkáltató informatikus munkatársa átvizsgálja és törli az esetlegesen az eszközökön található, nem üzleti adatokat, programokat. A munkafolyamatok folytonosságának biztosítása érdekében a munkáltató a kilépett munkavállaló munkavégzéssel összefüggő levelezését és munkahelyi dokumentumait archiválja és a mentési rend szerint tárolja. Az archív állományhoz kizárólag a munkáltató informatikus munkatársai rendelkeznek hozzáféréssel. Az archívumban történő keresés a Szervezet vezetőjének utasítása alapján, lehetőség szerint célzottan, a feladó és levél tárgya szerint történik.

A kilépett munkavállaló elektronikus levelezési címe, amennyiben és ameddig a munkafolyamatok folytonosságának biztosítása miatt szükséges, a Szervezet vezetőjének vagy a szervezeti egység vezetőjének elektronikus levélcímére átirányításra kerül. Amennyiben a munkafolyamatok folytonosságának biztosítás céljából szükséges, a kilépett munkavállaló számítástechnikai eszközökön tárolt munkahelyi dokumentumai, fájlok a Szervezet vezetőjének vagy a szervezeti egység vezetőjének átadásra kerülnek.

A Szervezet az adatkezeléshez fűződő jogos érdeke fennállásának megállapítása érdekében érdekmérlegelést készít különösen az alábbi adatkezelések esetén: munkahelyi megfigyelő rendszer, munkáltató által biztosított informatikai eszközök, gépjármű adatainak ellenőrzése, munkáltatói e-mail cím/fiók, internet és wifi használatának ellenőrzése (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 adatkezelés közérdekű feladat végrehajtásához, illetve közhatalmi jogosítvány gyakorlásához szükséges, az adatkezelésnek az uniós jogban vagy valamely tagállam jogában foglalt jogalappal kell rendelkeznie; egyetlen jogszabály jogalapul szolgálhat 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 Teresztenye Község 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/készülhetnek munkavállalói, ügyfelekkel kapcsolatos és szakmai, valamint egyedileg létrehozott kategóriával kapcsolatos adatkezelési tájékoztatók), 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 egy érvényes 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.

Adatkezelő ügyintézője a jelen szabályzat 7. vagy 8. mellékletei szerinti mintákat használhatja az érintett személyazonosságának megállapításának, az adatkezelő által kezelt adatok pontosságának utólagos ellenőrzése, bizonyítása érdekében.

4. Technikai és szervezési intézkedések

A Teresztenye Község 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 Teresztenye Község 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 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 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 magáncélú 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 fiók hozzáférését 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 hálózaton, 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.
- o Tilos az elektronikus információs rendszerek biztonsági beállításainak megváltoztatása, illetve a vírusellenőrző és Internet böngésző beállítások módosítása.
- o A kijelölt személy rendszeresen ellenőrzi, hogy a felhasználók számára biztosított az internet elérést lehetővé tevő szoftverek mentesek a komolyabb biztonsági hibáktól.
- o 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 visszaállítása 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 alapelveinek 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 Teresztenye Község 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 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 kimentő 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 behatásokról (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 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 Teresztenye Község Önkormányzata kizárólag olyan szoftvereket és kapcsolódó dokumentációt használ, amelyek megfelelnek a reájuk 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, csökkentve 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, és a továbbiakban 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,
- o a törlési mechanizmusokat az információ minősítési kategóriájával arányos erősségnek és sértetlenségnek megfelelően kell alkalmazni, biztosítva, hogy a megsemmisítési eljárások során a kimeneti információk tartalma helyreállíthatatlanul megsemmisüljön.
- Meghatározza és érvényesíti a felhasználó számítógépes szolgáltatásokhoz való hozzáférési jogosultságának hitelesítésére szolgáló jelszavak kezelésével kapcsolatos elvárásait:
 - o a munkaállomások, rendszerelemek, rendszerek hozzáféréséhez szükséges jelszavakat a jelszavak erősségének irányelve alapján kell megadni (figyelembe véve a jelszavak kompromittálásából adódó kockázatokat),
 - o 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 utalók vagy általános, szótári szavak (pl. „admin”, „password”), illetve amelyek gyári beállítású, alapértelmezett jelszavak,
 - o a munkaállomásokhoz, rendszerelemekhez, információs rendszerekhez kiadott kezdő jelszavakat kötelező az első bejelentkezés alkalmával megváltoztatni,
 - o a felhasználók és megbízott harmadik felek felelősek a személyes jelszavaik megfelelő védelméért és annak következményeiért, ha a jelszavaik mások által ismertté válnak,
 - o 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),
 - o a jelszavakat rendszeres időközönként cserélni kell (lehetőség szerint automatikusan kikényszerítve), illetve az elektronikus információs rendszer által kikényszerített, vagy az üzemeltetők által meghatározott időközönként,
 - o új jelszónak nem szabad az utolsó 5 régebbi közül egyiket sem megadni,
 - o a jelszavakat alapvetően tilos leírni,
 - o nem tehető a jelszó egy automatikus bejelentkezési folyamat részévé,
 - o tilos a felhasználóknak bejelentkezni olyan felhasználónévvel, melyet eredetileg nem nekik bocsátottak ki, és amelyek használatára nem jogosultak,
 - o 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,
 - o 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 meggátolása 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 beszerezett 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 Ibtv. 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;

adattfeldolgozás: az adatkezelő megbízásából vagy rendelkezése alapján eljáró adattfeldolgozó által végzett adatkezelési műveletek összessége;

adattfeldolgozó: 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 (15547633); 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 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 értékelésre, 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, megbízhatósághoz, 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.

Mellékletek

1. számú melléklet – Hozzáférés iránti kérelem (nem kötelező minta)
2. számú melléklet – Helyesbítés iránti kérelem (nem kötelező minta)
3. számú melléklet – Törlés iránti kérelem (nem kötelező minta)
4. számú melléklet – Adatkezelés korlátozása iránti kérelem (nem kötelező minta)
5. számú melléklet – Tiltakozásra vonatkozó nyilatkozat (nem kötelező minta)
6. számú melléklet – Érintetti tájékoztatás adatvédelmi incidensről (minta)
7. számú melléklet – Bemutatott okmányról készült feljegyzés (minta)
8. számú melléklet – Nyilatkozat a bemutatott hatósági okmányokról (minta)
9. számú melléklet – Feljegyzés szóban előterjesztett érintetti kérelemről (minta)
10. számú melléklet – Felhívás személyazonosság megerősítéséhez szükséges információk nyújtására
11. számú melléklet – Érintetti kérelem elutasítása (minta)
12. számú melléklet – Munkavállalói nyilatkozat számítástechnikai eszköz használatáról (minta)

1. számú melléklet – Hozzáférés iránti kérelem (minta)¹

Tisztelt Adatkezelő!

Alulírott, (név, születési hely és idő) mint a személyes adatok jogosultja², a(z) (adatkezelő megnevezése) mint Adatkezelő részére az alábbi

k é r e l m e t

terjesztem elő:

Kérem a Tisztelt Adatkezelő visszajelzését arra vonatkozóan, hogy személyes adataim kezelése folyamatban van-e, és ha ilyen adatkezelés folyamatban van, kérem a Tisztelt Adatkezelőt, hogy az általános adatvédelmi rendelet (GDPR) 15. cikk (1) és (2) bekezdése szerinti személyes adatokhoz és információkhoz való hozzáférést biztosítani szíveskedjék.

Kelt,, 20 év hó nap

.....

Kérelmező aláírása

¹ Használata nem kötelező

² Ha az adatkezelőnek megalapozott kétségei vannak a kérelmet benyújtó természetes személy kilétével kapcsolatban, további, az érintett személyazonosságának megerősítéséhez szükséges információk nyújtását kérheti.

2. számú melléklet – Helyesbítés iránti kérelem (minta)¹

Tisztelt Adatkezelő!

Alulírott, (név, születési hely és idő) mint a személyes adatok jogosultja, a(z) (adatkezelő megnevezése) mint Adatkezelő részére az alábbi

kérelmet

terjesztem elő:

Kérem a Tisztelt Adatkezelőt, hogy az általa kezelt és alább megjelölt pontatlan/hiányos személyes adataimat a jelen kérelemben meghatározottak szerint helyesbítse, illetőleg egészítse ki.

Jelenleg kezelt pontatlan személyes adat:

.....

Helyesbített, kiegészített személyes adat:

.....

A helyesbítés/kiegészítés igazolására szolgáló, a helyes személyes adatot tartalmazó dokumentum másolatát jelen nyilatkozatomhoz csatolom.²

Kérem a Tisztelt Adatkezelőt, hogy kérelmemben foglaltaknak helyt adni szíveskedjék.

Kelt,, 20 év hó nap

.....

Kérelmező aláírása

¹ Használata nem kötelező

² Szemrevételezés után megsemmisítésre kerül

3. számú melléklet – Törlés iránti kérelem (minta)¹

Tisztelt Adatkezelő!

Alulírott, (név, születési hely és idő) mint a személyes adatok jogosultja, a(z) (adatkezelő megnevezése) mint Adatkezelő részére az alábbi

kérelmet

terjesztem elő:

Kérem a Tisztelt Adatkezelőt, hogy az általa kezelt és alább megjelölt személyes adataimat indokolatlan késedelem nélkül valamennyi nyilvántartásából törölje.

Törölni kért személyes adat:
.....

Indokolás²

- a) A személyes adatokra már nincs szükség abból a célból, amelyből azokat gyűjtötték vagy más módon kezelték;
- b) Az érintett visszavonja az adatkezelés alapját képező hozzájárulását, és az adatkezelésnek nincs más jogalapja;
- c) Adatkezelő a személyes adatokat jogellenesen kezeli;
- d) A személyes adatokat az adatkezelőre alkalmazandó uniós vagy tagállami jogban előírt jogi kötelezettség teljesítéséhez törölni kell;
- e) A személyes adatok gyűjtésére közvetlenül gyermekeknek kínált, információs társadalommal összefüggő szolgáltatások vonatkozásában került sor.

Kérem a Tisztelt Adatkezelőt, hogy kérelmemben foglaltaknak helyt adni szíveskedjék.

Kelt,, 20 év hó nap

.....
Kérelmező aláírása

¹ Használata nem kötelező

² A megfelelő rész aláhúzendő

4. számú melléklet – Adatkezelés korlátozása iránti kérelem (minta)¹

Tisztelt Adatkezelő!

Alulírott, (név, születési hely és idő) mint a személyes adatok jogosultja, a(z) (adatkezelő megnevezése) mint Adatkezelő részére az alábbi

kérelmet

terjesztem elő:

Kérem a Tisztelt Adatkezelőt, hogy az általa kezelt és alább megjelölt személyes adataimra vonatkozóan végzett adatkezelést korlátozza.

Adatkezelés korlátozásával érintett személyes adat:
.....

Indokolás²

- a) Az érintett vitatja a személyes adat pontosságát;
- b) Az adatkezelés jogellenes, és az érintett ellenzi az adat törlését;
- c) Az adatkezelőnek már nincs szüksége a személyes adatra adatkezelés céljából, de az érintett igényli azokat jogi igényeinek előterjesztéséhez, érvényesítéséhez vagy védelméhez;
- d) Az érintett tiltakozik az adatkezelés ellen és az adatkezelő jogos indokai elsőbbségének megállapítása szükséges.

Kérem a Tisztelt Adatkezelőt, hogy kérelmemben foglaltaknak helyt adni szíveskedjék.

Kelt,, 20 év hó nap

.....
Kérelmező aláírása

¹ Használata nem kötelező

² A megfelelő rész aláhúzendó

5. számú melléklet – Tiltakozásra vonatkozó nyilatkozat (minta)¹

Tisztelt Adatkezelő!

Alulírott, (név, születési hely és idő) mint a személyes adatok jogosultja, a(z) (adatkezelő megnevezése) mint Adatkezelő részére az alábbi nyilatkozatot terjesztem elő:

A személyes adatok jogosultjaként

t i l t a k o z o m

az alább megjelölt személyes adataim Adatkezelő általi kezelése ellen.

Tiltakozással érintett személyes adat:.....
.....

Indokolás²

- a) Közvetlen üzletszerzés;
- b) Érintett saját helyzetével kapcsolatos ok³:.....
.....

Kérem a Tisztelt Adatkezelőt a nyilatkozatban foglaltak teljesítésére.

Kelt,, 20 év hó nap

.....
Nyilatkozatot tevő aláírása

¹ Használata nem kötelező

² A megfelelő rész aláhúzendó

³ Kérjük megjelölni

6. számú melléklet – Érintetti tájékoztatás adatvédelmi incidensről (minta)

(*érintett neve*)

(*érintett címe*)

Tárgy: tájékoztatás adatvédelmi incidensről

Tisztelt!

Alulírott, (szervezet képviselőjének neve) a(z) (adatkezelő megnevezése, székhelye) - a továbbiakban: „**Adatkezelő**” - képviselőként eljárva tájékoztatom, hogy Adatkezelőnél 20.....napján adatvédelmi incidens¹ történt. Az adatvédelmi incidens az Adatkezelő által Önről kezelt személyes adatokat is érintette, és az adatvédelmi incidens valószínűsíthetően magas kockázattal jár az Ön jogaira és szabadságaira.

Az adatvédelmi incidens jellege:

Az adatvédelmi incidensből eredő, valószínűsíthető következmények:

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

- a) megtett intézkedések:
- b) további tervezett intézkedések:

Tájékoztatom, hogy az alábbi elérhetőségeken felvilágosítás kérhető a bekövetkezett adatvédelmi incidenssel kapcsolatosan:

Adatvédelmi tisztviselő neve:

telefonszáma:

e-mail címe:

További kapcsolattartó neve:

telefonszáma:

e-mail címe:

Kelt,, 20 év hó nap

.....

aláírás

¹ „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.

7. számú melléklet – Bemutatott okmányról készült feljegyzés (minta)

Feljegyzés

Adatkezelő megnevezése:

Jelenlévő alkalmazottak neve, munkaköre¹:

1. Alkalmazott neve, munkaköre:

2. Alkalmazott neve, munkaköre:

Érintett neve, egyéb személyazonosító adata:

Feljegyzés kelte:

Érintett személyazonosságának megállapítása² és Adatkezelő által kezelt adatok pontossága érdekében az alábbi hatósági okmány(ok) kerültek szemrevételezésre:

Okmány megjelölése³:

Alulírottak megállapítjuk, hogy a mai napon ügyintézés céljából Adatkezelőnél megjelent természetes személy az Érintett, továbbá megerősítjük, hogy az Adatkezelő kezelésében lévő és az Érintett által közölt személyes adatok megegyeznek az Érintett által bemutatott hatósági okmány(ok)on szereplő személyes adatokkal.

K.m.f.

.....

1. Alkalmazott

.....

2. Alkalmazott

¹ A „négy szem elve” szerint két, az Adatkezelő alkalmazásában lévő személy jogosult megerősíteni az érintett személyazonosságát és a kezelt személyes adatok pontosságát az érintett által bemutatott hatósági okmány(ok) alapján.

² A polgárt saját maga azonosítása céljából csak egy azonosítási mód alkalmazására lehet kötelezni (1996. évi XX. törvény 4. § (2) bekezdés)

³ **Az okmányból nem rögzíthető személyes adat!**

8. számú melléklet – Nyilatkozat a bemutatott hatósági okmányokról (minta)

Nyilatkozat

Alulírott,

Név:

Egyéb személyazonosító adat:

nyilatkozom, hogy a mai napon a(z)-nál/nél *(adatkezelő megnevezése)*
megjelent természetes személy („Érintett”) a személyazonosságom megállapítása és igazolása céljából az
alábbi hatósági okmány(ok) kerültek bemutatásra¹:

Okmány megjelölése²:

Kelt,, 20 év hó nap

.....

aláírás

¹ A polgárt saját maga azonosítása céljából csak egy azonosítási mód alkalmazására lehet kötelezni
(1996. évi XX. törvény 4. § (2) bekezdés)

² **Az okmányból nem rögzíthető személyes adat!**

9. számú melléklet – Feljegyzés szóban előterjesztett érintetti kérelemről (minta)**Feljegyzés a szóban előterjesztett érintetti kérelemről**

Iktatószám:	
A feljegyzés készítésének helye:	
A feljegyzés készítésének ideje:	év hó nap
Ügyintéző neve, munkaköre:	
Érintetti kérelem előterjesztésének helye:	
Érintetti kérelem előterjesztésének módja:	Személyesen/Telefonon
Érintetti kérelem tárgya:	
Érintetti kérelem pontos meghatározása:	
Kérelmező neve:	
Kérelmező egyéb személyazonosító adata:	
Kérelmező státusza:	Érintett/Törvényes képviselő/Meghatalmazott
Kérelmező személyazonosító okmányának bemutatása ¹	Megtörtént/Nem történt meg
Kérelem teljesítésének kérelmező által kért formája, módja:	
A kérelem azonnali teljesítésére	Lehetőség van/Nincs lehetőség
Kérelem azonnali elutasításának ténye, annak indoka:	

K. m. f.

Ügyintéző aláírása

¹ A bemutatott okmányról feljegyzés vagy nyilatkozat szükséges.

10. számú melléklet – Felhívás személyazonosság megerősítéséhez szükséges információk nyújtására

(kérelmező neve)

(kérelmező elérhetősége)

Tárgy: felhívás személyazonosság megerősítéséhez szükséges információk nyújtására

Tisztelt Kérelmező!

A(z)(szervezet megnevezése, székhelye) mint adatkezelőhöz
20..... napján **elektronikus/postai úton/telefonon/személyesen benyújtott** érintetti
kérelmével összefüggésben, az Európai Parlament és a 2016. április 27-i (EU) 2016/679 rendelet 12. cikk (6)
bekezdése alapján, személyazonosságának megerősítéséhez további információk nyújtására hívom fel.

Személyazonosságát az alábbiak szerint kérem igazolni:

.....

Indokolás

.....

Érintetti kérelem csak abban az esetben teljesíthető, ha az adatkezelő minden kétséget kizáróan megállapította a kérelmező személyazonosságát. Az Európai Parlament és a 2016. április 27-i (EU) 2016/679 rendelet 12. cikk (6) bekezdése szerint, ha az adatkezelőnek megalapozott kétségei vannak a 15-21. cikk szerinti kérelmet benyújtó természetes személy kilétével kapcsolatban további, az érintett személyazonosságának megerősítéséhez szükséges információk nyújtását kérheti. Amennyiben a kérelmező nem vagy nem megfelelően tesz eleget jelen felhívásban foglaltaknak, és emiatt adatkezelő a kérelmező személyazonosságát nem tudja egyértelműen megállapítani, az érintetti kérelemben foglaltak semmilyen módon nem teljesíthetők.

Tájékoztatom, hogy az Európai Parlament és a 2016. április 27-i (EU) 2016/679 rendelete 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 (általános adatvédelmi rendelet, GDPR) 77. cikk (1) bekezdése és az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Infotv.) 60. § (2) bekezdése szerint jogosult a Nemzeti Adatvédelmi és Információszabadság Hatóságnál adatvédelmi hatósági eljárást lefolytatását kérelmezni jogainak érvényesítése érdekében.

Nemzeti Adatvédelmi és Információszabadság Hatóság elérhetőségei:

- Cím: 1055 Budapest, Falk Miksa utca 9-11.
- Levelezési cím: 1363 Budapest, Pf. 9.
- Telefonszám: +36 (1) 391-1400
- Fax: +36 (1) 391-1410
- E-mail: ugyfelszolgalat@naih.hu

Az általános adatvédelmi rendelet 79. cikk és az Infotv. 23. § (1) és (3) bekezdése szerint az érintett az adatkezelő, illetve - az adatfeldolgozó tevékenységi körébe tartozó adatkezelési műveletekkel összefüggésben - az adatfeldolgozó ellen bírósághoz fordulhat, ha megítélése szerint az adatkezelő, illetve az általa megbízott vagy rendelkezése alapján eljáró adatfeldolgozó a személyes adatait a személyes adatok kezelésére vonatkozó, jogszabályban vagy az Európai Unió kötelező jogi aktusában meghatározott előírások megsértésével kezeli. Az érintett választása szerint a per az alperes adatkezelő székhelye szerint illetékes törvényszék vagy az érintett felperes lakóhelye vagy a tartózkodási helye szerint

illetékes törvényszék előtt is megindítható. Az illetékes bíróságot megkeresheti a <https://birosag.hu/birosag-kereso> honlapon.

Kelt,, 20 év hó nap

.....

aláírás

11. számú melléklet – Érintetti kérelem elutasítása (minta)

(kérelmező neve)

(kérelmező elérhetősége)

Tárgy: érintetti kérelem elutasítása

Tisztelt Kérelmező!

Alulírott, (szervezet képviselőjének neve) a(z) (adatkezelő megnevezése, székhelye) - a továbbiakban: „**Adatkezelő**” - képviselőjében eljárva, az Európai Parlament és a 2016. április 27-i (EU) 2016/679 rendelet 12. cikk (4) bekezdése alapján tájékoztatom, hogy Adatkezelőnél 20.....napján **elektronikus/postai úton/telefonon/személyesen benyújtott érintetti kérelmemet elutasítom.**

A kérelmében foglaltaknak az alábbi indokok alapján nem teszek eleget:

.....

Tájékoztatom, hogy az Európai Parlament és a 2016. április 27-i (EU) 2016/679 rendelete 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 (általános adatvédelmi rendelet, GDPR) 77. cikk (1) bekezdése és az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Infotv.) 60. § (2) bekezdése szerint jogosult a Nemzeti Adatvédelmi és Információszabadság Hatóságnál adatvédelmi hatósági eljárást lefolytatását kérelmezni jogainak érvényesítése érdekében.

Nemzeti Adatvédelmi és Információszabadság Hatóság elérhetőségei:

- Cím: 1055 Budapest, Falk Miksa utca 9-11.
- Levelezési cím: 1363 Budapest, Pf. 9.
- Telefonszám: +36 (1) 391-1400
- Fax: +36 (1) 391-1410
- E-mail: ugyfelszolgalat@naih.hu

Az általános adatvédelmi rendelet 79. cikk és az Infotv. 23. § (1) és (3) bekezdése szerint az érintett az adatkezelő, illetve - az adatfeldolgozó tevékenységi körébe tartozó adatkezelési műveletekkel összefüggésben - az adatfeldolgozó ellen bírósághoz fordulhat, ha megítélése szerint az adatkezelő, illetve az általa megbízott vagy rendelkezése alapján eljáró adatfeldolgozó a személyes adatait a személyes adatok kezelésére vonatkozó, jogszabályban vagy az Európai Unió kötelező jogi aktusában meghatározott előírások megsértésével kezeli. Az érintett választása szerint a per az alperes adatkezelő székhelye szerint illetékes törvényszék vagy az érintett felperes lakóhelye vagy a tartózkodási helye szerint illetékes törvényszék előtt is megindítható. Az illetékes bíróságot megkeresheti a <https://birosag.hu/birosag-kereso> honlapon.

Kelt,, 20 év hó nap

.....

aláírás

12. számú melléklet – Munkavállalói nyilatkozat számítástechnikai eszköz használatáról (minta)

Munkavállalói¹ nyilatkozat

Információtechnológiai vagy számítástechnikai eszköz, rendszer munkavégzéssel összefüggő használatáról

Munkáltató megnevezése:

Munkavállaló neve:

Munkavállaló munkaköre:

Munkavállaló jelen nyilatkozat aláírásával tudomásul veszi és elfogadja, hogy a munkáltató által a munkavállaló részére munkavégzéséhez biztosított információtechnológiai vagy számítástechnikai eszközt, rendszert (együtt: számítástechnikai eszköz) munkavállaló kizárólag a munkaviszony teljesítése érdekében használhatja, **tilos a számítástechnikai eszköz magáncélú használata**. Tilos különösen a munkáltató által a munkavállaló részére biztosított elektronikus levélcím magáncélú használata, a számítástechnikai eszközön magáncélú képek, dokumentumok tárolása, az internet munkavégzéssel össze nem függő használata.

Munkavállaló a tiltás ellenére a munkáltató által biztosított számítástechnikai eszközön tárolt, magáncélú személyes adatokat köteles jelen nyilatkozat aláírását követően haladéktalanul, de legkésőbb 30 napon belül törölni.

Munkavállaló tudomásul veszi és elfogadja továbbá, hogy a munkaviszonya megszűnése esetén, a munkáltató által biztosított számítástechnikai eszköz átadás-átvételét megelőzően köteles a munkavégzéshez biztosított számítástechnikai eszközről törölni valamennyi, a számítástechnikai eszközön a tiltás ellenére tárolt magáncélú személyes adatot, beleértve különösen a magáncélú elektronikus levelezést, kép- és videófájlokat, dokumentumokat, internetes jelszavakat, keresési előzményeket.

Munkavállaló tudomásul veszi, hogy munkáltató az általa biztosított számítástechnikai eszköz használatára és annak ellenőrzésének szabályozására belső szabályzatot alkalmaz.

Kelt:

Munkavállaló aláírása

¹ Jelen nyilatkozat szerint munkavállalónak minősül a munka törvénykönyvéről szóló 2012. évi I. törvény, a közszolgálati tisztviselőkről szóló 2011. évi CXCV. törvény, a közalkalmazottak jogállásáról szóló 1992. évi XXXIII. törvény, az egészségügyi szolgálati jogviszonyról szóló 2020. évi C. törvény szerinti jogviszonyban és további munkavégzésre irányuló jogviszonyban álló személy.

Teresztenye Község Önkormányzata

Közterületi térfigyelő kamerarendszer adatvédelmi szabályzat

2011. évi CXII. törvény az információs önrendelkezési jogról
és az információszabadságról szerint

Önkormányzat közterület-felügyeletet vagy közterület-felügyelőt nem működtet

érvényes:

2023.09.01

jóváhagyta:


.....
Brogli Attila polgármester

1. Adatkezelő

Térfigyelő kamerarendszer tulajdonosa és üzemeltetője:

Név: Teresztenye Község Önkormányzata
Székhely: 3757 Teresztenye, Rákóczi Ferenc út 18
Polgármester: Brogli Attila
Adatvédelmi tisztviselő neve: GDPReg Kft.
Telefon: +36 48 463502
E-mail: adatvedelem@teresztenye.hu

A térfigyelő kamerarendszert a Kttv. 8. § (1) bekezdés alapján a Képviselő-testület döntésére a kezelésre és üzemeltetésre kijelölt, a települési önkormányzat alkalmazásában álló személy üzemelteti és kezeli.

A rendszer üzemeltetését, karbantartását végző adatfeldolgozó:

Név: BorsodWeb Kft.
Székhely: 3527 Miskolc, József A. u. 27. 2/1

2. Adatkezelésre vonatkozó jogforrások, egyéb szabályzatok

- Magyarország Alaptörvénye
- Közterület-felügyeletről szóló 1999. évi LXIII. törvény (továbbiakban: Kttv.)
- A Rendőrségről szóló 1994. évi XXXIV. törvény (továbbiakban: Rtv.)
- Magyarország helyi önkormányzatairól szóló 2011. évi CLXXXIX. törvény (továbbiakban: Mötv.)
- Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben (a továbbiakban: lbtv.)
- Az információs önrendelkezési jogról és információszabadságról szóló 2011. évi CXII. törvény (továbbiakban: Infotv.)
- Kapcsolódó főbb belső szabályzatok:
 - Adatvédelmi és adatbiztonsági szabályzat
 - Információbiztonsági szabályzat

3. Az adatkezelésre vonatkozó rendelkezések, a szabályzat, tájékoztató célja, hatálya

A térfigyelő kamerarendszer tulajdonosa és a térfigyelő kamerarendszer üzemeltetője - a Kttv. 7. § (3) bekezdésében és a 8. § (1) bekezdésben foglaltakra tekintettel – Teresztenye Község Önkormányzata (Adatkezelő). A Kttv. 8. § (1) bekezdése szerint, ha a települési önkormányzatnál közterület-felügyelet vagy közterület-felügyelő nem működik, a Kttv. 7. § (3) bekezdésében meghatározott képfeltevőt a jegyző, vagy a képviselő-testület által kijelölt, a települési önkormányzat alkalmazásában álló köztisztviselő is üzemeltetheti és kezelheti.

Jelen szabályzat fő célja, hogy Adatkezelő a létesített térfigyelő kamerarendszer adatkezeléssel kapcsolatos tevékenységek eljárásait rögzítse, elősegítve az információs önrendelkezési jognak az érvényesülését, és az érintetti jogok gyakorlását.

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

Adatkezelő 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 hatálya a közterületen, az önkormányzat közigazgatási területén elhelyezett és Adatkezelő által kezelt és üzemeltett térfigyelő kamerarendszerre terjed ki.

Jelen szabályzat a kiadás napján lép hatályba.

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) bekezdés 17. pontja).

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

A Kttfv. 7. § (3) bekezdése alapján a felügyelet közterületen, közbiztonsági, illetve bűnmegelőzési célból, bárki számára nyilvánvalóan észlelhető módon képfeltevőt helyezhet el, és felvételt készíthet.

Teresztenye Község Önkormányzata Képviselő-testülete 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 a **28/2023. (V.03.) képviselő-testületi határozatban döntött a képfeltevő elhelyezéséről.**

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

A képfeltevőt az Adatkezelő üzemelteti és kezeli. A képfeltevő által megfigyelt területre belépő személyek tájékoztatását elősegítő módon figyelemfelhívó jelzést, ismertetést helyez el 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). Adatkezelő a képfeltevők elhelyezéséről és a megfigyelt területre vonatkozó adatokról tájékoztatja a rendőrséget.

5. Értelmező rendelkezések

A szabályzat, tájékoztató alkalmazása során az egyes fogalmakon a következőket kell érteni, különösen az Infotv. 3. § 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 érintettre vonatkozó bármilyen adat.

Érintett: Bármely információ alapján azonosított vagy azonosítható természetes személy.

Adatkezelő: Az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely - törvényben vagy az Európai Unió kötelező jogi aktusában meghatározott keretek között - önállóan vagy másokkal együtt az adat kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja. 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.

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.

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

Adatkezelés korlátozása: A tárolt adat zárolása az adat további kezelésének korlátozása céljából történő megjelölése útján.

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

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.

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: Az adatbiztonság olyan sérelme, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisülését, elvesztését, módosulását, jogosulatlan továbbítását vagy nyilvánosságra hozatalát, vagy az azokhoz való jogosulatlan hozzáférést eredményezi.

6. A személyes adatok kezelésére vonatkozó elvek

Jogszerűség, tisztességes eljárás és átláthatóság: A személyes adat kizárólag egyértelműen meghatározott, jogszerű célból, jog gyakorlása és kötelezettség teljesítése érdekében kezelhető. Az adatkezelésnek minden szakaszában meg kell felelnie az adatkezelés céljának, az adatok gyűjtésének és kezelésének tisztességesnek és törvényesnek kell lennie.

Célhoz kötöttség, adattakarékosság, korlátozott tárolhatóság: Csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas. A személyes adat csak a cél megvalósulásához szükséges mértékben és ideig kezelhető.

Pontosság: Az adatkezelés során biztosítani kell az adatok pontosságát, teljességét és - ha az adatkezelés céljára tekintettel szükséges - naprakészségét, valamint azt, hogy az érintettet csak az adatkezelés céljához szükséges ideig lehessen azonosítani.

Integritás és bizalmas jelleg: Az adatkezelés során arra alkalmas műszaki vagy szervezési - így különösen az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisülésével vagy károsodásával szembeni védelmet kialakító - intézkedések alkalmazásával biztosítani kell a személyes adatok megfelelő biztonságát.

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 **hangtartalom nélküli képfelvételek** rögzítésének és felhasználásának további célja 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, illetve körözött személy vagy tárgy azonosítása érdekében.

8. A kezelt adatok köre, forrása

A képrögzítő eszközön a megfigyelt területre belépők képmása, tevékenysége, gépjármű típusa, forgalmi rendszám 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 levonhatók.

Amennyiben a kamerarendszer által rögzített adatok felhasználásra kerülnek, akkor személyes adatnak tekinthető az érintett magatartása is mint az érintettre vonatkozó következtetés.

Az Adatkezelő nem alkalmaz automatizált döntéshozatalt, kizárja az adatkezelési műveletei közül az adatok biometrikus felhasználását (pl. az arcfelismerés, mozgásfelismerés).

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

A térfigyelő kamerák, képfeltevők 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 térfigyelő rendszer személyes adatait az Infotv. 5. § (1) bekezdés a) pontja alapján, a Kfttv. 1. §-a és a 7. § (3) bekezdése rendelkezéseit figyelembe véve kezeli az Adatkezelő.

Jogalap: 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról 5. § a) - azt törvény vagy - törvény felhatalmazása alapján, az abban meghatározott körben, különleges adatnak vagy bűnügyi személyes adatnak nem minősülő adat esetén - helyi önkormányzat rendelete közérdeken alapuló célból elrendeli, ill. a település közterületei biztonságának és jogszerű használatának biztosítása a Magyarország helyi önkormányzatairól szóló 2011. évi CLXXXIX. törvény 13. § (1) bekezdés 17. pont.

10. Adatkezelés időtartama, a rögzített felvételek megismerése, továbbítása

Térfigyelő kamerarendszer képeinek megfigyelése:

A kamerarendszer által közvetített **élőkép megfigyelése nem történik**, a kamerarendszer által rögzített képfelvételek kizárólag a Kfttv-ben meghatározott esetekben kerülnek visszánézésre.

A kamerarendszer által továbbított személyes adatok kezelésére jogosultak:

- Képviselő-testület döntésére a kezelésre és üzemeltetésre kijelölt, a települési önkormányzat alkalmazásában álló személy

A kamerafelvételekbe a távoli betekintés tiltott.

Térfigyelő kamerarendszer képeinek rögzítése:

A közterületi térfigyelő 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, automatikusan törlésre kerülnek.

Rögzített felvételek visszánézése:

A térfigyelő 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 visszanézésére jogosultak:

- Képviselő-testület döntésére a kezelésre és üzemeltetésre kijelölt, a települési önkormányzat alkalmazásában álló személy

A visszanézett 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.

A Kfttv. alapján 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 győződni a képfelvételen látható személy és az érintetti jogával élni kívánó személy személyazonosságának egyezéséről, ennek érdekében a felvételekbe történő betekintés az érintett személyes megjelenéséhez kötött, illetve a hozzáférési jog másolat kérésű gyakorlása - személyes jelenlét nélkül- a személy egyértelmű beazonosíthatósága mellett gyakorolható.

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 kamerarendszert üzemeltető személy tudomására jutott rendkívüli eseményt tartalmazó felvételek esetén a felvétel rögzítésétől számított két munkanapon belül a közterületi térfigyelő kamerarendszert üzemeltető, kezelő személy 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:

A rögzített felvételekbe betekintést a harmadik fél részére a következő szabályok alapján biztosít az Adatkezelő.

- Az eljárásra jogosult szerv, hatóság megkeresésére: a Kfttv-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 közigazgatási hatósági eljárásban az eljáró hatóság megkeresésére továbbítható a felvétel, ha a megkereső hatóság a megkeresésben az eljárás tárgyát, ügyszámát és a rögzített felvétellel bizonyítandó ténnyel megjelöli. A rögzített felvétel továbbítására irányuló megkeresést meg kell tagadni, ha a felvétel a megkeresésben meghatározott tény bizonyítására alkalmatlan.

Adattovábbítás céljából adatmentést a jogosult személy végezhet.

A rögzített felvétel továbbítása:

- Az eljárásra jogosult szerv, hatóság megkeresésére: a Kfttv-ben rögzített felhasználási célból megkeresésre a rendőrség, a nemzetbiztonsági szolgálat, a hivatásos katasztrófavédelmi szerv részére továbbítja, 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 továbbíthatja, ha a megkeresésben vagy adatkérésben megjelölésre került az eljárás tárgya, ügyszáma és a rögzített felvétellel bizonyítandó tény. A közigazgatási hatósági eljárásban az eljáró hatóság megkeresésére továbbítható a felvétel, ha a megkereső hatóság a megkeresésben az eljárás tárgyát, ügyszámát és a rögzített felvétellel bizonyítandó tényt megjelöli. A rögzített felvétel továbbítására irányuló megkeresést meg kell tagadni, ha a felvétel a megkeresésben meghatározott tény bizonyítására alkalmatlan.
- Az Rtv. alapján a rendőrség konkrét kérésre fix IP-címről férhet hozzá a felvételekhez nyilvántartási kötelezettség mellett, amit az Adatkezelő ellenőriz.
- A felvételen szereplő személy számára: ha jogainak érvényesítésére kérelmet nyújtott be, 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 30 napig.

Ha a rögzített felvételt Adatkezelő az eljárásra jogosult szerv, hatóság megkeresésére vagy a felvételen szereplő személy kérelmére továbbította, a felvételt a továbbítással egyidejűleg törölni kell.

Adatkezelő a felvétel kezelése során köteles megtenni az ahhoz szükséges szervezési, technikai és egyéb adatbiztonsági intézkedéseket, hogy az érintett személy személyes adatait, így különösen magántitkait és magánéletének körülményeit illetéktelen személy tudomására jutásától megóvja. Szükség esetén ki kell takarni az egyéb személyes adatokat. Adatkezelőnek biztosítani kell továbbá, hogy a felvételen szereplő személy - a felvétel törlésének időpontjáig - megtekinthesse a róla készült felvételt.

A rendszer üzemeltetését, karbantartását végző adatfeldolgozó hatásköre:

Adatfeldolgozó az adatfeldolgozási szerződés keretein belül, illetőleg a szerződés teljesítése céljából Adatkezelő írásbeli utasítása szerint jogosult a felvételekhez és naplófájlokhoz hozzáférni, adatkezelési és technikai műveletben közreműködni; így különösen a felvételen szereplő személyek, személyes adatok, területek kitakarása, maszkolása, adatmentésben közreműködés.

11. Szervezési, technikai és egyéb adatbiztonsági intézkedések

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 képfelvevő 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.

Adatkezelő és tevékenységi körében az adatfeldolgozó a kezelt személyes adatok megfelelő szintű biztonságának biztosítása érdekében az érintettek alapvető jogainak érvényesülését az adatkezelés által fenyegető - így különösen az érintettek különleges adatainak kezelésével járó - kockázatok mértékéhez igazodó műszaki és szervezési intézkedésekkel biztosítja:

- az adatkezeléshez használt eszközök (adatkezelő rendszer) jogosulatlan személyek általi hozzáféréseinek megtagadását,
- az adathordozók jogosulatlan olvasásának, másolásának, módosításának vagy eltávolításának megakadályozását,
- az adatkezelő rendszerbe a személyes adatok jogosulatlan bevitelének, valamint az abban tárolt személyes adatok jogosulatlan megismerésének, módosításának vagy törlésének megakadályozását,
- az adatkezelő rendszerek jogosulatlan személyek általi, adatátviteli berendezés útján történő használatának megakadályozását,
- azt, hogy az adatkezelő rendszer használatára jogosult személyek kizárólag a hozzáférési engedélyben meghatározott személyes adatokhoz férjenek hozzá,
- azt, hogy ellenőrizhető és megállapítható legyen, hogy a személyes adatokat adatátviteli berendezés útján mely címzettnek továbbították vagy továbbíthatják, illetve bocsátották vagy bocsáthatják rendelkezésére,
- azt, hogy utólag ellenőrizhető és megállapítható legyen, hogy mely személyes adatokat, mely időpontban, ki vitt be az adatkezelő rendszerbe,
- a személyes adatoknak azok továbbítása során vagy az adathordozó szállítása közben történő jogosulatlan megismerésének, másolásának, módosításának vagy törlésének megakadályozását,
- azt, hogy üzemzavar esetén az adatkezelő rendszer helyreállítható legyen, valamint
- azt, hogy az adatkezelő rendszer működőképes legyen, a működése során fellépő hibákról jelentés készüljön, továbbá a tárolt személyes adatokat a rendszer hibás működtetésével se lehessen megváltoztatni.

A kezelt elektronikus adatok védelmére továbbá az *Adatvédelmi és adatbiztonsági szabályzatban*, valamint az *Informatikai biztonsági szabályzatban* foglaltaknak megfelelően kell biztosítani.

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.

11.1. Naplózás, automatizált adatkezelési rendszer (elektronikus napló)

A személyes adatokkal elektronikus úton végzett adatkezelési műveletek jogszerűségének ellenőrizhetősége céljából Adatkezelő automatizált adatkezelési rendszerben (a továbbiakban: *Elektronikus napló*) rögzíti:

- az adatkezelési művelettel érintett személyes adatok körének meghatározását,

- az adatkezelési művelet célját és indokát,
- az adatkezelési művelet elvégzésének pontos időpontját,
- az adatkezelési műveletet végrehajtó személy megjelölését,
- a személyes adatok továbbítása esetén az adattovábbítás címzettjét.

Amennyiben a térfigyelő kamerarendszer műszakilag nem képes arra, hogy elektronikus naplóban rögzítse az adatkezelési művelet célját és indokát, valamint a személyes adatok továbbítása esetén az adattovábbítás címzettjét, Adatkezelő az Infotv. 25/F. § (1) bekezdés b) és e) pontjaiban foglalt kötelezettségét a személyes adatokkal elektronikus úton végzett adatkezelési műveletek jogszerűségének ellenőrzése céljából, az elektronikus napló kiegészítéseként papír alapú nyilvántartást (a továbbiakban: *Elektronikus naplót kiegészítő nyilvántartás*) vezet az adatkezelési műveletek céljáról és indokáról (lásd 3. sz. melléklet).

Az *Elektronikus naplóban* és az *Elektronikus naplót kiegészítő nyilvántartásban* rögzített adatok kizárólag az adatkezelés jogszerűségének ellenőrzése, az adatbiztonsági követelmények érvényesítése, továbbá büntetőeljárás lefolytatása céljából ismerhetők meg és használhatóak fel, melyekhez a Nemzeti Adatvédelmi és Információszabadság Hatóság, továbbá jelen bekezdésben meghatározott célból jogszabályban meghatározott tevékenységet folytató személy és szervezet részére - azok erre irányuló kérelmére - az Adatkezelő hozzáférést biztosít, abból részükre adatot továbbít.

Adatkezelő felelősségi körébe tartozik, hogy az adatkezelési műveletekhez felhasznált automatizált adatkezelési rendszer teljesíteni tudja az Infotv. 25/F. §-ban elvárt követelményeket, olyan térfigyelő rendszert üzemeltessenek, amely alkalmas az elektronikus naplózásra.

11.2. Jelszó (tudás) alapú hitelesítés

A kamerarendszer által kezelt személyes adatok megismerésére csak a hozzáférésre engedélyezetttek jogosultak. Adatkezelő felelőssége, hogy az adatkezelési műveletekhez felhasznált automatizált adatkezelési rendszer a szükséges mértékben naplózza a személyes adatok hozzáféréseit.

A munkavégzéshez tartozó tevékenységi köröket és az azokhoz szükséges jogosultságokat Adatkezelő vezetője határozza meg. 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 jelszavak a felhasználó számítógépes szolgáltatásokhoz való hozzáférési jogosultságának hitelesítésére szolgálnak. Adatkezelő felelősségi körébe tartozik, hogy az adatkezelési műveletekhez felhasznált eszköz (szerver, rögzítő) alkalmas legyen a felhasználók és a felhasználók által végzett tevékenységek/ szerepkörök egyedi azonosítására és hitelesítésére.

A jelszavakra vonatkozó minimális elvárások:

1. A jelszónak minden felhasználó számára bármikor szabadon megváltoztathatónak kell lenni
2. A jelszavakat ne tárolják visszafejthető titkosítással
3. A biztonságos jelszó minimális hossza legalább 8 karakter, kisbetűt, nagybetűt, számot és speciális karakter tartalmaznia kell
4. A jelszó ne legyen kívülálló számára kitalálható, ne tartalmazzon a felhasználó személyére utaló információkat, nem tartalmazhatja a felhasználó nevét
5. Ha a felhasználó azt gyanítja, hogy jelszavát valaki megismerte, azonnal le kell azt cserélnie és a jelszó felfedése nélkül jelentenie kell Adatkezelőnek

6. A jelszavakat nem szabad felírni, papíron tárolni. Amennyiben ez elkerülhetetlen, gondoskodni kell a jelszó biztonságos helyen zárt borítékban történő tárolásáról
7. A felhasználói munkaállomásokat úgy kell beállítani, hogy azok téltlenség esetén maximum 15 perc után zárolják a munkaállomást, amit csak jelszóval lehessen feloldani
8. Mielőtt az ügyintéző elhagyja a munkaállomást, zárolnia kell azt
9. A felhasználói jelszavakat kötelezően 90 naponként meg kell változtatni

11.3. Szerepkörök, jogosultság nyilvántartás

A kamerarendszer által közvetített képek megfigyelésére, a rögzített felvételek kezelésére csak a hozzáférésre engedélyezettek jogosultak. Adatkezelő vezetője a térfigyelő kamerarendszer kezelése és üzemeltetése során, a megfelelő szintű adatbiztonsági intézkedések érvényesülése érdekében, az adatkezelési műveletek jogszerűségének ellenőrzése céljából meghatározza a különböző felhasználók adatkezelésével kapcsolatos feladatellátásukhoz kapcsolódó jogosultságokat. Az egyes felhasználók számára beállított különböző adatkezelési műveletekre vonatkozó jogosultságokról Adatkezelő a 2. melléklet szerint naprakész nyilvántartást vezet (a továbbiakban: *Jogosultság nyilvántartás*).

11.4. A szerver, szerverhelyiség fizikai védelme

A térfigyelő kamerarendszer eszközeit zárható, megfelelő fizikai védelemmel ellátott szerverhelyiségben vagy ennek hiányában rackszekrényben kell elhelyezni.

A térfigyelő kamerarendszer szerverhelyisége, a szervernek/rögzítőnek helyt adó helyiség, illetőleg az operátori szoba (továbbiakban szerverhelyiség) kockázatokkal arányos fizikai biztonságáról (nyílászárók védelme, vagyonvédelmi rendszer, távfelügyelet) Adatkezelő köteles gondoskodni.

Valamennyi belépési lehetőséget, pl. ajtót és ablakot azon időszak alatt, amikor ott személyek nem tartózkodnak, lezárt állapotban kell tartani. A helyiségek szabályos zárásáért a beosztás szerint dolgozók vagy a helyiséget utoljára elhagyó felelős.

11.5. A szerverhelyiségbe történő belépések felügyelete

Adatkezelőnél szerverhelyiség nincs kialakítva, a szerver zárható rackszekrényben található Adatkezelő székhelycímén. Adatkezelő a rackszekrénynek helyt adó irodahelyiséget zártan tartja, oda Adatkezelő képviselője által jóváhagyott, folyamatosan aktualizált Belépési jogosultak nyilvántartásban engedélyezett személyek jogosultak belépni a meghatározott korlátozásokkal (lásd 4. sz. melléklet). A belépésre jogosultakat írásban kell rögzíteni, a jogosultságot megadónak és az átvevőnek aláírásával igazolni kell a jogosultságot. A listát rendszeresen, legalább éves gyakorisággal tervezetten felül kell vizsgálni, a belépésre már nem jogosultakat el kell távolítani. Adatkezelő képviselője intézkedik a belépési jogosultság megszűnését követően a kiosztott belépési jogosultságot igazoló dokumentum, kulcs visszavonásáról, illetve a nyilvántartás aktualizálásáról. Az állandó belépési jogosultsággal nem rendelkező személyek esetében csak nyilvántartás, felügyelet és kíséret mellett lehetséges a belépés és a bent tartózkodás.

Adatkezelő felelősségi körébe tartozik megfelelő kulcskezelési szabályzat, gyakorlat kialakítása. A rackszekrény folyamatos zárásáról gondoskodni kell, a kulcsot nem lehet a zártan tartani. A rackszekrény kulcsát Adatkezelő az 5. melléklet szerinti (*Használatra kiadott kulcsok nyilvántartása*) dokumentáltan adja át az őrzésre és használatra jogosultnak. A hivatali kulcsokat csak munkaidőben vagy a korlátozásnak megfelelően, azon túl az Adatkezelő vezetőjének engedélyével lehet használni. Az átvevő a dokumentáció aláírásával a kulcs átvételét, valamint a kulcs őrzésére, kezelésére vonatkozó szabályok megismerését is

igazolja. A kulcsot átvevő köteles a jogosultság visszavonását követően a kulcsot visszaadni, s az átadást aláírásával igazolni. Az átvevő kötelessége a kulcs megőrzéséről gondoskodni, a kulcsot harmadik személy számára nem adhatja át, anyagi-fegyelmi és büntetőjogi felelősséggel tartozik a rábízott kulcs(ok) használatáért, a kulcs elvesztése tényét vagy bármely szabálytalanság észlelését haladéktalanul jelenteni köteles.

11.6. Megőrzési idő

Az Elektronikus naplóban és az Elektronikus naplót kiegészítő nyilvántartásban rögzített adatokat a kezelt adat törlését követő 10 évig kell megőrizni.

Adatkezelő kötelezettsége gondoskodni olyan adatmentési rendszer kialakításáról, ami biztosítja, hogy a térfigyelő kamerarendszer szerveréről/rögzítőjéről készülő adatmentésekből az Infotv. 25/F. § (4) bekezdésben foglalt kötelezettségének megfelelően a 11.1. Naplózás pontban meghatározott elektronikus adatok, naplófájlok az adatok törlését követő 10 évig visszaállíthatóak legyenek.

A Jogosultság nyilvántartás és Belépési Napló, valamint a Használatra kiadott kulcsok nyilvántartása megőrzési ideje 10 év.

11.7. Az adathordozó szállítása

Adatkezelő felelős az adathordozó szállítása közben a személyes adatok jogosulatlan megismerésének, másolásának, módosításának vagy törlésének megakadályozásáért. Adatkezelőnek a kiszállításra engedélyezett adathordozóról nyilvántartást (jegyzőkönyvet, átvételi elismervényt) kell írni vagy elektronikus nyilvántartást vezetni, amely egyértelműen tartalmazza az adathordozó jellemzőit és a kiadással járó felelőségeket. Az adathordozó visszaszolgáltatásakor a visszavevőnek meg kell győződnie arról, hogy az megfelel a kiadáskori állapotának.

Az adathordozó használata során tilos:

- az adathordozót illetéktelen személynek átengedni,
- az adathordozó közelében folyadékot, éghető anyagot, illetve felette, alatta vagy rajta az eszköz rendeltetésétől eltérő anyagot, tárgyat elhelyezni és tárolni és
- az adathordozót – a kiszállításra engedélyezett hordozható infokommunikációs eszközök kivételével – a telepítési helyéről elmozdítani és elvinni Adatkezelő engedélye és közreműködése nélkül.

12. Érintettek jogai

Érintett jogosult arra, hogy törvényben meghatározott jogainak érvényesítése érdekében Adatkezelőhöz forduljon.

Adatkezelő az érintett jogai gyakorlására irányuló kérelmét az annak beérkezésétől számított legfeljebb huszonöt napon belül elbírálja és döntéséről az érintettet írásban vagy elektronikus úton értesíti. A kérelem beérkezésének napja a határidőbe nem számít bele.

Az Infotv-nek megfelelően az érintettek az alábbi főbb jogokat gyakorolhatják:

Előzetes tájékoztatáshoz való jog:

Az érintett jogosult arra, hogy Adatkezelő által kezelt, személyes adatai vonatkozásában az adatkezelést megelőzően tájékoztatást kapjon az adatkezeléssel kapcsolatos alábbi tényekről: az adatkezelő, illetve adatfeldolgozó megnevezése és elérhetősége; az adatvédelmi tisztviselő neve és elérhetősége; az adatkezelés célja; az adatkezelés jogalapja; a kezelt személyes adatok megőrzésének időtartama; az

adattovábbítás címzettjei; a kezelt személyes adatok gyűjtésének forrásai; az érintettet az Infotv. alapján megillető jogok, valamint azok érvényesítésének módja.

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

Adatkezelő a képfelvevők 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).

Hozzáféréshez való jog:

Az érintett jogosult arra, hogy kérelmére személyes adatait és azok kezelésével összefüggő információkat Adatkezelő a rendelkezésére bocsássa, így különösen: az adatkezelést maga az adatkezelő, illetve megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó végzi-e, a kezelt személyes adatok forrását, az adatkezelés célját és jogalapját, a kezelt személyes adatok körét, a kezelt személyes adatok továbbítása esetén az adattovábbítás címzettjeinek - ideértve a harmadik országbeli címzetteket és nemzetközi szervezeteket - körét, a kezelt személyes adatok megőrzésének időtartamát, ezen időtartam meghatározásának szempontjait, az érintettet az Infotv. alapján megillető jogok, valamint azok érvényesítése módjának ismertetését, profilalkotás alkalmazásának esetén annak tényét és az érintett személyes adatainak kezelésével összefüggésben felmerült adatvédelmi incidensek bekövetkezésének körülményeit, azok hatásait és az azok kezelésére tett intézkedéseket.

Helyesbítéshez való jog:

Az érintett jogosult arra, hogy kérelmére Adatkezelő vagy megbízásából adatfeldolgozó által kezelt személyes adatokat Adatkezelő haladéktalanul pontosítsa, helyesbítse, illetőleg, ha az adatkezelés céljával összeegyeztethető, kiegészítse akkor, ha a kezelt személyes adatok pontatlanok, helytelenek vagy hiányosak.

Adatkezelő mentesül a fenti kötelezettség alól, ha a pontos, helytálló, illetve hiánytalan személyes adatok nem állnak rendelkezésre és azokat az érintett sem bocsátja a rendelkezésre, vagy az érintett által rendelkezésre bocsátott személyes adatok valódisága kétséget kizáróan nem állapítható meg.

A helyesbítéshez való jog nem gyakorolható a felvételeken szereplő személyes adatok vonatkozásában.

Az adatkezelés korlátozásához való jog:

Adatkezelő köteles az érintett kérelmére vagy az Infotv. 19. §-ában meghatározott esetekben az érintett személyes adatai kezelésének korlátozására. Az adatkezelés korlátozásának időtartama alatt a korlátozással érintett személyes adatokkal Adatkezelő a tároláson túl egyéb adatkezelési műveletet kizárólag az érintett jogos érdekének érvényesítése céljából vagy törvényben, nemzetközi szerződésben, illetve az Európai Unió kötelező jogi aktusában meghatározottak szerint végezhet.

Törléshez való jog:

Adatkezelő az érintett kérelmére, valamint az Infotv. 20. §-a szerint, az alább meghatározott esetekben törli az érintett személyes adatait.

Adatkezelő haladéktalanul törli az érintett személyes adatait, ha az adatkezelés jogellenes, az érintett az adatkezeléshez adott hozzájárulását visszavonja vagy a személyes adatainak törlését kérelmezi (kivéve, ha az adatkezelést törvény vagy helyi önkormányzat rendelete közérdeken alapuló célból rendeli el, illetve az adatkezelés az érintett vagy más személy létfontosságú érdekeinek védelméhez, valamint a személyek

életét, testi épségét vagy javait fenyegető közvetlen veszély elhárításához vagy megelőzéséhez szükséges és azzal arányos, különleges adat esetén ha az törvényben kihirdetett nemzetközi szerződés végrehajtásához feltétlenül szükséges és azzal arányos, vagy azt az Alaptörvényben biztosított alapvető jog érvényesítése, továbbá a nemzetbiztonság, a bűncselekmények megelőzése, felderítése vagy üldözése érdekében vagy honvédelmi érdekből törvény elrendeli), az adatok törlését jogszabály, az Európai Unió jogi aktusa, a Nemzeti Adatvédelmi és Információszabadság Hatóság (Hatóság) vagy a Bíróság rendelte el, továbbá az Infotv. 19. § (1) bekezdés b)-d) pontjában meghatározott időtartam eltelt.

Jogorvoslathoz/panasztételhez való jog

Amennyiben Adatkezelő által folytatott adatkezeléssel kapcsolatban kérdése, panasza merül fel, vagy az előzőekben ismertetett jogait kívánja gyakorolni, úgy az érintett közvetlenül fordulhat Adatkezelőhöz, vagy adatvédelmi tisztviselőjéhez a jelen tájékoztatóban megadott elérhetőségeken.

Az érintett kezdeményezheti a Hatóság vizsgálatát az adatkezelői intézkedések jogszerűségének vizsgálata céljából, ha Adatkezelő az érintett előzőekben felsorolt jogainak érvényesítését korlátozza vagy a kérelmét elutasítja; továbbá a Hatóság adatvédelmi hatósági eljárásának lefolytatását kérelmezheti, amennyiben megítélése szerint Adatkezelő a személyes adatainak kezelése során megsértette a személyes adatok kezelésére vonatkozó jogszabályi előírásokat.

Az érintett az Adatkezelő – illetve az adatfeldolgozó tevékenységi körébe tartozó adatkezelési műveletekkel összefüggésben – az adatfeldolgozó ellen bírósághoz fordulhat, ha megítélése szerint Adatkezelő, illetve az általa megbízott vagy rendelkezése alapján eljáró adatfeldolgozó a személyes adatok kezelésére vonatkozó, jogszabályban vagy az Európai Unió kötelező jogi aktusában meghatározott előírások megsértésével kezeli. A pert az érintett - választása szerint - a lakóhelye vagy tartózkodási helye szerint illetékes törvényszék előtt is megindíthatja.

Nemzeti Adatvédelmi és Információszabadság Hatóság elérhetőségei:

1055 Budapest, Falk Miksa utca 9-11., Postacím: 1363 Budapest, Pf. 9.

Telefonszám: +36 1 391 1400; fax: +36 1 391 1410; e-mail: ugyfelszolgalat@naih.hu; honlap: www.naih.hu

Verzió: v4

**TERESZTENYE KÖZSÉG ÖNKORMÁNYZATA ÜZEMELTETÉSÉBEN LÉVŐ
KÖZTERÜLETI TÉRFIGYELŐ KAMERÁK
ELHELYEZÉSÉRE, A MEGFIGYELT TERÜLETRE VONATKOZÓ ADATOK**

kamera típus jelmagyarázat:

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

F = Fix

R = rendszámfelismerő

Sorszám	Kamera telepítési helyének címe (utca, házszám)	Kamera típus	Megfigyelt közterület
01	Teresztenye, Rákóczi út 28-30.	F	A kamera a Rákóczi út 30. számától a 24. számig látja közterületet, magánterületek kimaszkolva.
02	Teresztenye, Rákóczi út 28-30.	F	A kamera Rákóczi út és a Kossuth út találkozását látja az Önkormányzati garázsig, magánterületek kimaszkolva.
03	Teresztenye, Kossuth út 27.	F	A kamera a Kossuth út 27. számától a Kossuth út 4. számig látja a közterületet, magánterületek kimaszkolva.
04	Teresztenye, Kossuth út 27.	F	A kamera a Kossuth út 27. számától az Önkormányzati garázsig látja a közterületet, magánterületek kimaszkolva.
05	Teresztenye, Kossuth út 13.	F	A kamera a Kossuth út 13. számától a buszmegálló előtti területig látja a közterületet, magánterületek kimaszkolva.
06	Teresztenye, Kossuth út 13.	F	A kamera a Kossuth út 13. számától a Kossuth út 21. számig (vízcsap) látja a közterületet, magánterületek kimaszkolva.
07	Teresztenye, Bevezető út patak hid	F	A kamera a Teresztenyére bevezető útszakaszt, helységnév táblát, illetve a díszteret látja, magánterületek kimaszkolva.
08	Teresztenye, Bevezető út patak hid	F	A kamera a patakhídtól a szennyvíz átemelőig látja a közterületet, magánterületek kimaszkolva.
09	Teresztenye, Rákóczi út 18.	F	A kamera a Rákóczi út 18. szám előtti területtől a Rákóczi út 08. szám előtti elágazásig látja a közterületet, magánterület kimaszkolva.
10	Teresztenye, Rákóczi út 18.	D	A kamera a Rákóczi út 18. számától a 2. hrsz.-ú területig látja a közterületet, magánterületek kimaszkolva.

.....
dátum

.....
Brogli Attila

ELEKTRONIKUS NAPLÓT KIEGÉSZÍTŐ NYILVÁNTARTÁS

3. melléklet

#	Műveletet végző személy	Időpont (év, hónap, nap, óra, perc)	MŰVELET			Hatósági megkeresés tárgya, ügyszáma	Érintett / Adattovábbítás címzettje
			megnevezése (belekintés, törlés, másolás, továbbítás)	célja	indoka		

HASZNÁLATRA KIADOTT KULCSOK NYILVÁNTARTÁSA

Önkormányzat neve: Teresztenye Község Önkormányzata

Helyiség, bejárat/ajtó, kulcs megnevezése:

A kulcsok őrzésére vonatkozó szabályok:

A hivatali kulcsokat csak munkaidőben vagy a korlátozásnak megfelelően, azon túl a polgármester engedélyével lehet használni. Az átvevő az aláírásával a kulcs átvételét, valamint a kulcs őrzését, kezelésére vonatkozó szabályok megismerését is igazolja. A kulcsot átvevő köteles a jogosultság visszavonását követően a kulcsot visszaadni, s az átadást aláírásával igazolni. Az átvevő kötelessége a kulcs megőrzéséről gondoskodni, a kulcsot harmadik személy számára nem adhatja át. anyagi-fegyelmi és büntetőjogi felelősséggel tartozik a rábízott kulcs(ok) használatáért, a kulcs elvesztése tényét vagy bármely szabálytalanság észlelését haladéktalanul jelenteni köteles.

sor- szám	KIADÁS						VISSZAVÉTEL		megjegyzés
	átvevő neve	átvevő munkaköre	időbeni korlátozás	átvétel időpontja	átvevő aláírása	engedélyező aláírása	időpontja	visszavevő aláírása	

K – korlátlan kulcshasználat H – korlátozás hivatali időre

A Teresztenye településen található kamerák látószögének leírása.

01 kamera (Rákóczi út 28-30)

A kamera a Rákóczi út 30. számától a 24. számig látja közterületet, magánterületek kimaszkolva.

02 kamera (Rákóczi út 28-30)

A kamera Rákóczi út és a Kossuth út találkozását látja az Önkormányzati garázsig, magánterületek kimaszkolva.

03 kamera (Kossuth út 27)

A kamera a Kossuth út 27. számától a Kossuth út 4. számig látja a közterületet, magánterületek kimaszkolva.

04 kamera (Kossuth út 27)

A kamera a Kossuth út 27. számától az Önkormányzati garázsig látja a közterületet, magánterületek kimaszkolva.

05 kamera (Kossuth út 13)

A kamera a Kossuth út 13. számától a buszmegálló előtti területig látja a közterületet, magánterületek kimaszkolva.

06 kamera (Kossuth út 13)

A kamera a Kossuth út 13.számától a Kossuth út 21. számig (vízcsap) látja a közterületet, magánterületek kimaszkolva.

07 kamera (Patakhíd)

A kamera a Teresztenyére bevezető útszakaszt, helységnév táblát, illetve a díszteret látja, magánterületek kimaszkolva.

08 kamera (Patakhíd)

A kamera a patakhídtól a szennyvíz átemelőig látja a közterületet, magánterületek kimaszkolva.

09 kamera (Önkormányzati hivatal)

A kamera a Rákóczi út 18. szám előtti területtől a Rákóczi út 08. szám előtti elágazásig látja a közterületet, magánterület kimaszkolva.

10 kamera (Önkormányzati hivatal)

A kamera a Rákóczi út 18. számától a 2. hrsz.-ú területig látja a közterületet, magánterületek kimaszkolva.

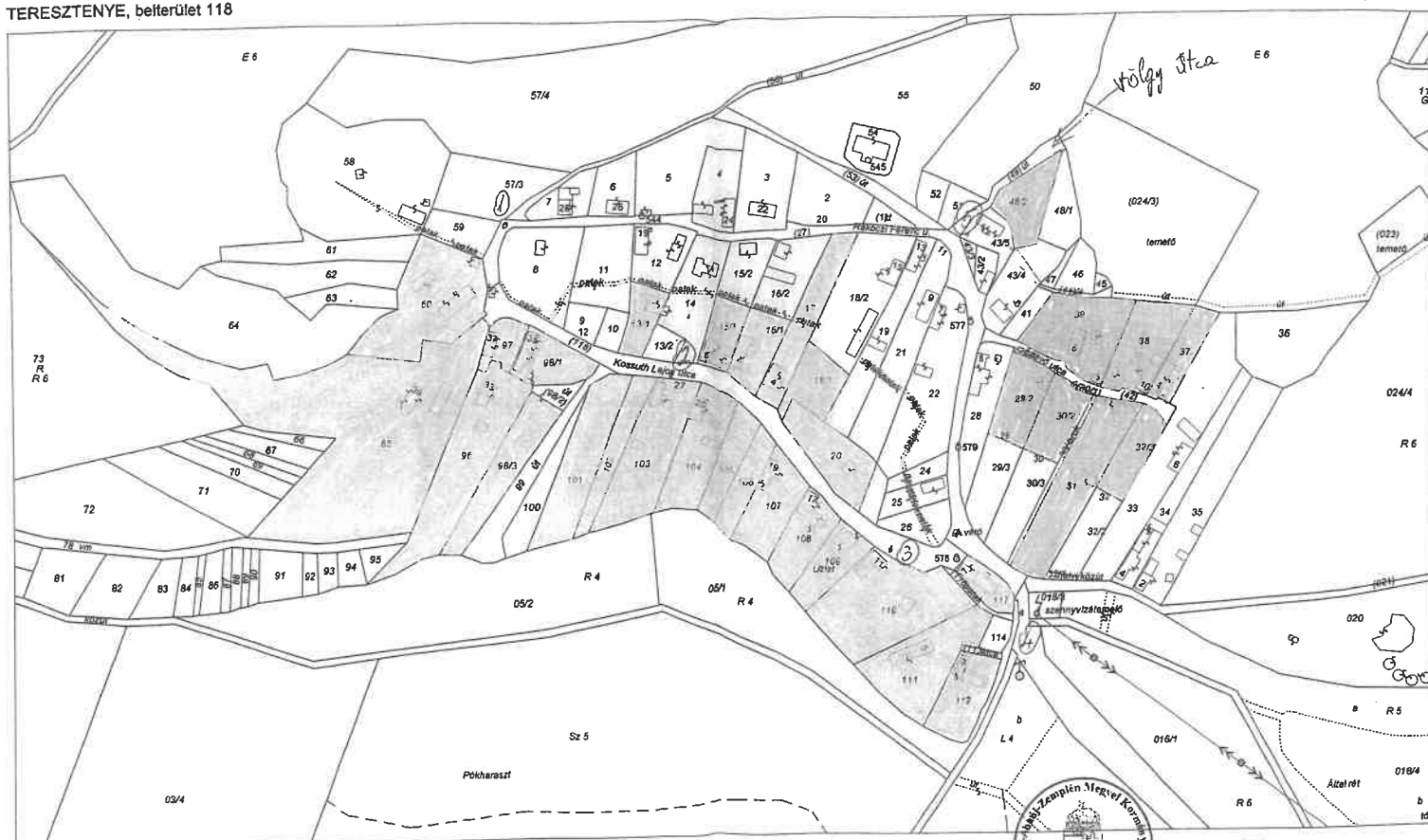
B-A-Z. Vármegyei Kormányhivatal Földhivatali Főosztály
3780 Edelény István király útja 52/A.

Szelvénytípus: 97-224-41
TERESZTENYE, belterület 118

Térképmásolat - Teljes

Iktatószám: 1/23/2023

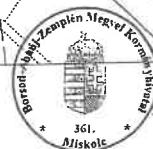
Vetület: EOV
Méretarány: 1:2000



A térképmásolat a kiadást megelőző napig megegyezik az ingatlan-nyilvántartási térképi adatbázis tartalmával.

A térképmásolat méreteit levételére nem használhatók.

3780 Edelény, 2023. február 8.



Deák Hilda

Adatfeldolgozási szerződés

amely létrejött egyrészről:

Teresztenye Község Önkormányzata

Székhely: 3757 Teresztenye Rákóczi Ferenc út 18.

Adószám: 15547633-1-05

Képviselő: Brogli Attila

mint **Adatkezelő,**

másrészről

BORSODWEB Internet Szolgáltató Kft.

Székhely: 3527 Miskolc, József Attila utca 27. II. em. 1. ajtó

Cégjegyzékszám: 05-09-007640

Adószám: 11845850-2-05

Képviselő: Czifra Zsolt László ügyvezető

mint **Adatfeldolgozó**

a továbbiakban együtt: **Felek** között az alulírott helyen és napon, az alábbi feltételekkel:

Előzmények

1. Adatkezelő és Adatfeldolgozó 2023. szeptember 01. napjától hatályos szerződést kötött Teresztenye településen üzemeltetett térfigyelő kamerarendszer karbantartása, üzemeltetése tárgyban (a továbbiakban: **Alapszerződés**).
2. Tekintettel arra, hogy az Alapszerződés teljesítése során személyes adatok kezelésére, feldolgozására kerül sor, jelen megállapodással Felek rögzítik az Adatkezelő és az Adatfeldolgozó közötti jogviszonyt, valamint az Adatfeldolgozó tevékenységét az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Infotv.) 25/C.-25/D. § szerint.

A szerződés tárgya

3. Adatfeldolgozó az Alapszerződés hatálya alatt az Alapszerződésben meghatározott feladatokat lát el Adatkezelő részére a jelen Adatfeldolgozási szerződésben részletezett adatvédelmi feltételekkel.
4. Felek rögzítik, hogy Adatfeldolgozó Adatkezelő utasítása szerint, illetőleg az Alapszerződés szerződésszerű teljesítése érdekében a jelen Adatfeldolgozási szerződésben meghatározott célokból az 5. pontban meghatározott adatokat kezeli, valamint hogy kizárólag e célokhoz kötve, a jelen Adatfeldolgozási szerződésben foglaltak szerint az adatokkal kapcsolatos tevékenységet végez.
5. Adatfeldolgozó adatfeldolgozási tevékenysége során kezelt, a Felek között létrejött Alapszerződés teljesítéséhez szükséges személyes adatok típusa és az érintettek köre:
 - térfigyelő kamerarendszer naplófájlokkal összefüggő személyes adatok; érintett a műveletet végző, jogosult személy;
 - képfelvételekkel összefüggő személyes adatok (így különösen képmás, viselkedés, gépjárműre vonatkozó adatok); érintett a felvételen megjelenő személy, gépjármű tulajdonos.

Teljesítés

6. Felek rögzítik, hogy Adatfeldolgozó az Alapszerződésben meghatározott feladatok ellátása során a teljesítéshez szükséges és elégséges személyes adatok feldolgozását végzi.
7. Adatkezelő felelősséget vállal, hogy Adatfeldolgozónak átadott, vagy hozzáférhetővé tett személyes adatok gyűjtése jogszerűen történt, azok kezelésére, valamint adatfeldolgozásba adására jogosult.
8. Adatkezelő az Adatfeldolgozó szerződéses kötelezettségeinek teljesítése érdekében, az Adatfeldolgozó számára átadja, vagy hozzáférhetővé teszi az Alapszerződésben meghatározott feladatok teljesítéséhez szükséges és elégséges személyes adatokat. Amennyiben jelen Adatfeldolgozási szerződés teljesítéséhez szükséges, Adatkezelő a szükséges mértékben hozzáférést biztosít Adatfeldolgozó részére azon rendszerekhez, adatokhoz, amelyek szükségesek az adatfeldolgozói feladatok ellátásához.
9. Adatfeldolgozó nem köteles vizsgálni, hogy Adatkezelő kizárólag olyan személyes adatokhoz ad hozzáférést, melyek adatfeldolgozása az Alapszerződés teljesítéséhez elengedhetetlenül szükségesek.

10. Adatfeldolgozó a személyes adatokat kizárólag Adatkezelő írásbeli utasítása alapján kezeli - beleértve a személyes adatoknak valamely harmadik ország vagy nemzetközi szervezet számára való továbbítását is -, kivéve akkor, ha az adatkezelést az Adatfeldolgozóra alkalmazandó uniós vagy tagállami jog írja elő; ebben az esetben erről a jogi előírásról az Adatkezelőt az adatkezelést megelőzően értesíti, kivéve, ha az Adatkezelő értesítését az adott jogszabály fontos közérdekből tiltja. Felek rögzítik, hogy Adatfeldolgozó a személyes adatokat csak Adatkezelő írásbeli utasítása alapján, meghatározott célból és jogalapból továbbíthatja. Felek rögzítik, hogy Adatfeldolgozó a személyes adatokat törvényi kötelezettség hiányában harmadik ország vagy nemzetközi szervezet számára nem továbbíthatja, továbbítás esetén minden ebből eredő kárért teljes anyagi felelősséggel tartozik.
11. Adatkezelő által adott utasításokért az Adatkezelő felel. Adatfeldolgozó köteles Adatkezelőt késedelem nélkül, az utasítás végrehajtása előtt figyelmeztetni, ha Adatkezelő célszerűtlen vagy szakszerűtlen utasítást ad, továbbá ha az utasítás közvetlenül alkalmazandó uniós jogi aktus vagy jogszabály adatvédelmi rendelkezéseibe ütközik, vagy sérti az Adatfeldolgozóra irányadó adatvédelmi rendelkezéseket.
12. Adatfeldolgozó nem végezhet a jelen Adatfeldolgozási szerződésben rögzített feladatok ellátásához nem szükséges, valamint uniós szabályban vagy jogszabályban meghatározott adatfeldolgozói feladatok körét meghaladó tevékenységet, az adatkezelést érintő érdemi döntést nem hozhat, a tudomására jutott adatokat kizárólag Adatkezelő rendelkezései szerint dolgozhatja fel, saját céljára adatfeldolgozást nem végezhet, valamint Adatkezelő rendelkezései szerint köteles az adatokat tárolni, illetve megőrizni. Felek rögzítik, hogy az adatkezelést érintő érdemi döntésnek tekinthető különösen az adatkezelés céljának meghatározása, az adatkezelés időtartamának meghatározása, az adatkezelés során alkalmazott eszközöknek kiválasztása, adatok megismerésére jogosult személyek körének meghatározása, az adatok továbbításáról való döntés, az érintettek tájékoztatására vonatkozó kötelezettség teljesítése.
13. Adatkezelő utasításaitól eltérő, vagy Adatkezelő utasítása nélküli eljárásból fakadó jogsértésekért – amennyiben erre az Adatkezelőt késedelem nélkül, az utasítás végrehajtása előtt Adatfeldolgozó nem figyelmeztette – Adatfeldolgozó felelős.
14. Adatfeldolgozó az Adatkezelő előzetesen írásban tett eseti vagy általános felhatalmazása nélkül további adatfeldolgozót nem vehet igénybe. Az általános írásbeli felhatalmazás esetén Adatfeldolgozó tájékoztatja Adatkezelőt minden olyan tervezett változásról, amely további adatfeldolgozók igénybevételét vagy azok cseréjét érinti, ezzel biztosítva lehetőséget Adatkezelőnek arra, hogy ezekkel a változtatásokkal szemben kifogást emeljen. Felek rögzítik, hogy Adatfeldolgozó további adatfeldolgozót az Infotv. rendelkezései szerint és az abban meghatározott feltételek teljesítése mellett vehet igénybe.

Jogok és kötelezettségek

15. Felek rögzítik, hogy Adatfeldolgozó az adatkezelés jellegének figyelembevételével megfelelő technikai és szervezési intézkedésekkel a lehetséges mértékben köteles segíteni Adatkezelőt abban, hogy teljesíteni tudja kötelezettségét az érintett jogainak gyakorlásához kapcsolódó kérelmek megválaszolása tekintetében. Felek rögzítik, hogy érintetti jogok maradéktalan érvényesülése érdekében Felek között ezzel összefüggésben csak Adatkezelőtől érkező írásbeli vagy elektronikus módon közölt kommunikáció tekinthető joghatályosnak, abban az esetben is, ha az érintett szóbeli kérelemmel élt Felek felé.
16. Adatfeldolgozó nem jogosult közvetlenül az érintettől kérelmet befogadni, Adatfeldolgozó kötelezettsége az érintett Adatkezelőhöz irányítására vonatkozó tájékoztatásra korlátozódik.
17. Adatkezelő előzetes egyeztetést követően jogosult ellenőrizni az Adatfeldolgozó jelen szerződés szerinti tevékenységének végrehajtását, Adatfeldolgozó indokolatlan zavarása nélkül, a vonatkozó biztonsági intézkedések betartásával.
18. Adatfeldolgozó segíti Adatkezelőt a személyes adatok védelmére vonatkozó kötelezettségek teljesítésében, figyelembe véve az adatkezelés jellegét és Adatfeldolgozó rendelkezésére álló információkat.
19. Adatfeldolgozó az adatvédelmi incidenst köteles az arról való tudomásszerzését követően indokolatlan késedelem nélkül, legkésőbb az észleléstől számított 24 órán belül írásban bejelenteni Adatkezelőnek. Felek rögzítik, hogy Adatfeldolgozó nem jogosult adatvédelmi incidens esetén bejelentéssel élni a NAIH felé, továbbá az érintettek tájékoztatása is Adatkezelő kötelezettsége.
20. Adatvédelmi incidens észlelése esetén Adatfeldolgozónak törekednie kell arra, hogy minden szükséges és tőle elvárható módon segítse Adatkezelőt az adatvédelmi incidens bejelentés megtételében. Ennek érdekében Adatkezelő felé történő értesítésnek – amennyiben lehetséges – legalább az alábbi tartalmi elemeket kell magában foglalnia:

- a. ismertetni kell az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát;
- b. közölni kell a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;
- c. ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket;
- d. ismertetni kell az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

Együttműködés, kapcsolattartás

- 21. Felek a jelen Adatfeldolgozási szerződés teljesítése érdekében együttműködési kötelezettséget vállalnak, melynek keretében kötelesek a szerződés teljesítését befolyásoló minden lényeges körülményt egymással haladéktalanul közölni. Felek kijelentik, hogy az adatfeldolgozással kapcsolatban együttműködési kötelezettségeiknek az általában elvárható módon tesznek eleget, az adatfeldolgozás hibátlan teljesítésének, az adatfeldolgozás biztonsági követelményeinek megtartásának és az érintettek magánszférájának tiszteletben tartásának érdekében. Adatfeldolgozó köteles az Adatkezelőt a jelen szerződés teljesítéséhez kapcsolódó tevékenységéről folyamatosan, a szükséges mértékben tájékoztatni, a feladat teljesítése során Adatkezelővel együttműködni.
- 22. Felek rögzítik, hogy egymás között a kapcsolatot az adatfeldolgozással kapcsolatos utasításokra vonatkozóan írásos módon (beleértve az elektronikus utat) tartják. Az értesítés elmulasztásából eredő következményekért a mulasztó Fél felelős.
- 23. Adatfeldolgozó köteles Adatkezelő rendelkezésére bocsátani minden olyan információt, amely az adatfeldolgozó igénybevételeire vonatkozó jogi rendelkezéseknek való megfelelés igazolásához szükséges.

Adatbiztonság, titoktartás

- 24. Adatkezelő, illetőleg a szerződésből eredő feladatai tekintetében Adatfeldolgozó köteles megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek az adatvédelmi szabályok érvényre juttatásához szükségesek.
- 25. Felek kijelentik, hogy tevékenységük során Infotv.-ben és minden egyéb adatvédelmi ágazati jogszabályban előírtaknak, az adatvédelmi szabályoknak és joggyakorlatnak megfelelően járnak el, a hatályos jogszabályok előírásait betartják, illetve az adatvédelemhez kapcsolódó fontosabb nemzetközi ajánlásokat is figyelembe veszik, ennek keretében gondoskodnak arról, hogy a tárolt adatokhoz belső rendszeren keresztül vagy közvetlen hozzáférés útján kizárólag az arra feljogosított személyek, és kizárólag az adatkezelés céljával összefüggésben férjenek hozzá; gondoskodnak a felhasznált eszközök szükséges, rendszeres karbantartásáról, fejlesztéséről; az adatokat tároló eszközt megfelelő fizikai védelemmel ellátott zárt helyiségben helyezik el, gondoskodnak annak fizikai és logikai védelméről is.
- 26. Adatfeldolgozó vállalja, hogy az Adatkezelő által rendelkezésre bocsátott Adatvédelmi és adatbiztonsági szabályzatot, tájékoztatót megismeri, annak irányadó rendelkezéseit elfogadja, és az adatfeldolgozási tevékenysége vonatkozásában magára nézve kötelezőnek ismeri el.
- 27. Adatfeldolgozó a jelen szerződésben meghatározott feladatok ellátása érdekében megfelelő ismerettel és gyakorlattal rendelkező személyeket köteles alkalmazni. Köteles továbbá gondoskodni az általa alkalmazott személyek felkészítéséről, a vonatkozó Európai Uniói adatvédelmi szabályok és jogszabályi rendelkezések, adatkezelési folyamatok (beleértve Adatkezelő irányadó rendelkezéseit is), valamint a jelen szerződésben foglalt kötelezettségek tekintetében. Adatfeldolgozó kötelezettséget vállal arra, hogy további - adatkezelésben érintett - adatfeldolgozó igénybevétele esetén Adatkezelő irányadó, az al-adatfeldolgozó tevékenységét érintő, a szerződés teljesítéséhez szükséges rendelkezéseit vele megismerteti és betartatja.
- 28. Adatfeldolgozó tevékenysége során biztosítja azt, 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.
- 29. Adatfeldolgozót teljes kártérítési felelősség terheli a jelen Adatfeldolgozási szerződésben meghatározott kötelezettségek bármely megsértéséért, valamint az Adatfeldolgozónál munkavégzésre irányuló jogviszonyban álló személyek és Adatfeldolgozó közreműködői által történő, jelen szerződésben foglaltakat, illetőleg bármely hatályos jogszabályt érintő megsértéséért.

30. Feleket a jelen szerződés teljesítése keretében tudomására jutott minősített, valamint személyes adat tekintetében büntetőjogi felelősség terheli. Egyéb bizalmas információk átadására vagy nyilvánosságra hozatalára egyik Fél sem jogosult, kivéve azon rendelkezéseket, amelyek nyilvánosságra hozatalát Adatkezelő vagy az Adatfeldolgozó vonatkozásában jogszabály írja elő, így különösen a közérdekű és közérdekből nyilvános adatokra vonatkozó jogi előírások. Nyilvánosságra hozatalnak minősül a jogosulatlan harmadik személlyel történő közlés is.
31. A minősített adatokra vonatkozó titoktartási kötelezettség Feleket jelen szerződés megszűnése esetén a minősítés tartamáig kötelezi. Más, a szerződéssel kapcsolatban keletkezett titok és egyéb, a teljesítés során keletkezett bizalmas információk tekintetében a Feleket időkorlátra nélkül, illetőleg a titokjogosult rendelkezése szerint terheli titoktartási kötelezettség.
32. Felek megállapodnak, hogy a jelen szerződéssel és annak teljesítésével kapcsolatos, vagy valamely Félre, különösen annak működésére, szervezetére vonatkozó információ, illetőleg minden olyan tény, adat, terv, okirat, dokumentum, eljárás bizalmas információnak minősül, amely valamelyik Fél tevékenységével összefügg.
33. Adatfeldolgozó kötelezettséget vállal arra, hogy Adatkezelő által átadott, a teljesítéshez kapcsolódó iratokról, dokumentumokról másolatot, kivonatot csak az Adatkezelő előzetes engedélyével készít, és ezen iratokba harmadik személy részére betekintést nem ad, illetve semmilyen más módon nem hozza harmadik személy tudomására azok tartalmát.
34. A titoktartási kötelezettség megsértéséből, illetve az adatok jogosulatlan nyilvánosságra hozatalából származó hátrányok, valamint az ezek kiküszöböléséhez szükséges költségek, ideértve mind a vagyoni, mind a nem vagyoni kár megtérítését – az egyéb felelősségén túl – azt a Felet terhelik, akinek a jogosulatlan nyilvánosságra hozatal tekintetében felelőssége fennáll.

Szerződés hatálya, módosítása, megszűnése

35. **Felek rögzítik, hogy jelen Adatfeldolgozási szerződés a Felek között létrejött Alapszerződés fennállásával azonos időtartamra kötöttik, az Alapszerződésnek elválaszthatatlan részét képezi.** Felek - tekintettel az Infotv. 25/D. § (1) bekezdésében foglaltakra, mely szerint az adatfeldolgozó által végzett adatkezelést szerződésnek vagy más jogi aktusnak kell szabályoznia – jelen Adatfeldolgozási szerződés önálló megszüntetésének a jogát kizárják. Felek rögzítik, hogy jelen Adatfeldolgozási szerződés megszűnik, amennyiben a közöttük létrejött Alapszerződés bármilyen oknál fogva megszűnik.
36. A jelen szerződés módosítása kizárólag írásban a Felek közös megállapodása alapján érvényes.
37. Felek rögzítik, hogy jelen Adatfeldolgozási szerződés valamely rendelkezésének érvénytelensége nem érinti a szerződés egészének érvényességét. Felek az együttműködési kötelezettségük teljesítése során az érvénytelen szerződéses kikötések esetén kötelesek olyan szabályozást kidolgozni, mely az érvénytelen szerződéses rendelkezésekkel elérni kívánt célt megvalósítja. A szerződés részbeni érvénytelensége esetén az egész szerződés akkor dől meg, ha feltehető, hogy a Felek azt az érvénytelen rész nélkül nem kötötték volna meg.
38. Felek rögzítik, hogy a jelen Adatfeldolgozási szerződés és az Alapszerződés személyes adatok kezelésére - beleértve az adatfeldolgozást is – vonatkozó rendelkezései közötti ellentmondás esetén jelen Adatfeldolgozási szerződés az irányadó.

Elszámolás a szerződés megszűnése esetén

39. Felek rögzítik, hogy az adatfeldolgozás megszűnését követően Adatfeldolgozó az Adatkezelő utasításának megfelelően köteles Adatkezelő vagy az általa kijelölt más adatfeldolgozó részére átadni minden általa feldolgozott, a részére átadott személyes adatot, dokumentációt és azok másolatait, valamint Adatkezelő számára a jelen szerződés szerinti kötelezettségei teljesítése kapcsán készített anyagot. Az átadás-átvételt a Felek képviselőinek dokumentálniuk kell.
40. Amennyiben az adatkezelés jogszerűen nem folytatható, Adatfeldolgozó köteles az Adatkezelő rendelkezése szerint az adatok megsemmisítéséről gondoskodni, ennek tényét jegyzőkönyvben rögzíteni, a jegyzőkönyvet az Adatkezelő részére átadni, vagy elektronikus formában tárolt adatok esetén informatikai rendszerében dokumentálni.
41. Adatfeldolgozó Adatkezelő vagy a felügyeleti hatóság kérésére lehetővé teszi az adatfeldolgozó rendszerének rendelkezésére bocsátását az adatok megsemmisítésével kapcsolatos intézkedések ellenőrzése céljából.

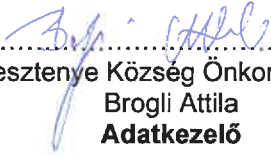
Egyéb rendelkezések

42. A jelen szerződésben nem szabályozott kérdésekben a Polgári Törvénykönyvről szóló 2013. évi V. törvény, az Infotv. és az ágazati jogszabályok vonatkozó rendelkezései irányadók.

Jelen Adatfeldolgozási szerződést a Felek alulírott helyen és időpontban, elolvasás és az abban foglaltak megértése után, mint szerződéses akaratukkal mindenben megegyezőt aláírják.

Kelt.:

Kelt.:


Teresztenye Község Önkormányzata
Brogli Attila
Adatkezelő

.....
BORSODWEB Internet Szolgáltató Kft.
Czifra Zsolt László
Adatfeldolgozó

ADATVÉDELMI HATÁSVIZSGÁLATI KIEGÉSZÍTŐ DOKUMENTÁCIÓ

TERESZTENYE KÖZSÉG ÖNKORMÁNYZATA

TÉRFIGYELŐ KAMERÁS ADATKEZELÉS

I. Hatásvizsgálat szükségességének meghatározása	
1. Kötelező hatásvizsgálat alá tartozik-e az adatkezelés	Igen, a NAIH által közzétett hatásvizsgálati lista 14. pontja szerint: „Módszeres megfigyelés. Érintettek nagyszámú és módszeres megfigyelése jellemzően közterületeken vagy nyilvános helyeken történő kamerarendszerek, drónok felhasználásával, illetve bármely más új technológia használatával (Wi-Fi tracking, Bluetooth tracking, testkamera).” Teresztenye Község Önkormányzata térfigyelő kamerák elhelyezéséről döntött Teresztenye közterületein.
2. Vizsgálat célja	A hatásvizsgálat célja, hogy az adatkezelő a tervezett adatkezelés megkezdését megelőzően felmérje, hogy a tervezett adatkezelés annak körülményeire, így különösen céljára, az érintettek körére, az adatkezelési műveletek során alkalmazott technológiára tekintettel várhatóan milyen hatásokat fog gyakorolni az érintetteket illető alapvető jogok érvényesülésére (Infotv. 25/G. § (1) bekezdés)
3. Vizsgálat terjedelme:	A vizsgálat kiterjed az adatkezelés hatókörének körülményeinek és céljának, ideértve az egyes adatkezelési műveletek terjedelmének, a személyes adatok tárolásának módjának, megőrzési idejének meghatározására. A hatásvizsgálat a Privacy Impact Assessment (PIA) szoftverrel dokumentált.
4. Vizsgálatban közreműködő személyek	A hatásvizsgálatot dokumentálja: GDPR Reg Kft. A hatásvizsgálati dokumentációban szereplő adatok, információk forrása: Teresztenye Község Önkormányzata (és közvetetten: a BorsodWeb Kft.). A GDPR Reg Kft. a BorsodWeb Kft-től közvetlenül nem kér be adatot. Az adatvédelmi hatásvizsgálathoz szükséges, annak során Teresztenye Község Önkormányzata által átadatok, információk e-mailben dokumentáltak.
5. Megjegyzés	Az adatkezelés az Infotv. 2. § (3) bekezdése alapján az Infotv. hatálya alá tartozik. Az adatkezelés jogalapja az Infotv. 5. § (1) bekezdés a) pontja, az adatkezelés a Mötv. és a Kfttv. felhatalmazása alapján valósul meg. Az Infotv. nem ismeri az érdekmérlegelés fogalmát, azonban az adatvédelmi tisztviselő jelen dokumentációba foglalja az érdekmérlegelés egyes elemeit annak érdekében, hogy az adatkezelő és az érintett jogainak ütköztetését megfelelően dokumentálja, kiegészítve az adatvédelmi hatásvizsgálati dokumentációt.
II. Adatkezelés célja, kezelendő személyes adatok, tervezett idő	
1. Cél meghatározása	Az adatkezelés célját törvény határozza meg; Magyarország helyi önkormányzatairól szóló 2011. évi CLXXXIX. törvény (Mötv.) 13. § (1) bekezdés 17. pontjában meghatározott, a helyi közügyek, valamint a

	helyben biztosítható közfeladatok körében ellátandó, Teresztenye település közbiztonságában való közreműködés mint helyi önkormányzati feladat ellátása. Adatkezelő Teresztenye Község Önkormányzata e feladatkörében eljárva, a közterület-felügyeletről szóló 1999. évi LXIII. törvény (Kttfv.) 7. § (3) bekezdése szerint a közterületen közbiztonsági, illetve bűnmegelőzési célból döntött a bárki számára nyilvánvalóan észlelhető módon történő képfelvételek elhelyezéséről. Teresztenye 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 növelése.
2. Jogos érdekek meghatározása	Adatkezelő jogos érdeke a település lakosságának jólétét és biztonságát a lehető leghatékonyabb módon garantálni, figyelemmel az átlátható gazdálkodás elvére és a gazdaságos működés követelményére. Az adatkezelésre törvény ad felhatalmazást az adatkezelőnek, az adatkezelés részleteit is törvény szabályozza. Teresztenye településének 70-80 %-a idős, 60 év feletti lakos, akiknek biztonságérzetét a kamerarendszer kiépítése jelentősen növeli.
3. Kezelt adatok	A megfigyelt területre belépő személyek képmása, használt gépjármű és forgalmi rendszám, valamint a kamerarendszer üzemeltetéséhez szükséges jogosultak adatai, naplófájlok. Személyes adatnak is minősülő képfelvételek kerülnek rögzítésre, tárolásra, a felvételen beazonosítható természetes személyek jelenhetnek meg különböző mozgást, magatartást megvalósítva, amelyből akár közvetett vagy közvetlen következtetések is levonhatók.
4. Adatkezelés ideje	A képfeltevő eszközzel rögzített videofelvételek megőrzési ideje a Kttfv. 7. § (7) bekezdés b) pontja szerint a rögzítést követő 30 nap. A naplófájlok és jogosultságok megőrzési ideje az Infotv. 25/F. § (4) bekezdése szerint 10 év.
5. Megjegyzés	Adatkezelő jelen érdekmérlegelésben a képfeltevő üzemeltetéséhez szükséges járulékos adatokra, így a naplófájlok kezelésére nem tér ki, tekintettel arra, hogy a naplózás követelményét az Infotv. 25/F. §-a kötelezően előírja a személyes adatok elektronikus úton végzett adatkezelési műveletek jogszerűségének ellenőrizhetősége céljából.
III. Alternatív megoldások, módszerek	
6. Alternatív módszerek, megoldások (kevésbé korlátozó lehetőségek)	A település lélekszáma nem indokolja, az önkormányzat gazdaságos működése nem teszi lehetővé közterület-felügyelet működtetését mint alternatív megoldást.
IV. Adatkezelő érdekének azonosítása	
7. Szükségesség meghatározása – milyen előnyökkel jár az adatkezelés	
a) konkrét helyzet tényszerű leírása	Adatkezelő Teresztenye Község Önkormányzata Borsod-Abaúj-Zemplén vármegyében található zsáktelepülés. A rendőrség hivatalos adatai szerint a vármegyében regisztrált bűncselekmények száma az

	országos átlaghoz képest magas, ezért kiemelten fontos a közbiztonság, bűnmegelőzés szerepe, melyben a Mőtv. 13. § (1) bekezdés 17. pontja alapján az önkormányzatoknak is felelősséget kell vállalniuk. A településen főleg időskorúak élnak, a 60 év felettiek aránya kb. 70-80%. A település lakosai között felmérést végzett adatkezelő a kamerarendszer kiépítésének szükségessége kérdésében, a lakosok nagy aránya támogatta a rendszer kiépítését. A képfelvevők kezelésére és üzemeltetésére a képviselő-testület által az önkormányzat alkalmazásában álló munkavállaló került kijelölésre. Élőkép megfigyelése nem történik, a képfelvételek kizárólag a Kfttv-ben foglalt esetekben kerülnek megtekintésre, szükség esetén továbbításra.
b) miért és mennyiben jelenti az érintettek magánszférájának a korlátozását az adatkezelés	A személyes adatok védelme alkotmányos védelem alá tartozik. Alapvető elvárás, hogy mindenki számára lehetővé és ellenőrizhetővé kell tenni az adatkezelés egész útját, vagyis mindenkinek joga van tudni, hogy ki, hol, mikor, milyen célra használja a személyes adatát. A Polgári Törvénykönyv (Ptk.) 2:48. § védi a képmáshoz és hangfelvétellel való jogot, melynek alapján képmás és hangfelvétel elkészítéséhez és felhasználásához az érintett személy hozzájárulása szükséges. Nincs szükség az érintett hozzájárulására a felvétel elkészítéséhez és az elkészített felvétel felhasználásához tömegfelvétel és nyilvános közéleti szereplésről készült felvétel esetén. Vékás Lajos és Gárdos Péter által szerkesztett Nagykomentár a Polgári Törvénykönyvről szóló 2013. évi V. törvényhez a képmáshoz és hangfelvétellel való jognál akképpen fogalmaz, hogy „a képmáshoz és a hangfelvétellel való jog az emberi személyiség külső megnyilvánulását védi. Az ember külső megjelenése a személyiség belső sajátosságait vetíti ki, ezáltal az egyén megkülönböztetésének nélkülözhetetlen eszköze. A képmás és a hangfelvétel közvetlenül a személyiség azonosítására szolgál. A Ptk. a képmás és hangfelvétel védelmének személyiségi jogi oldalát, magánjogi oltalmát szabályozza. A képmás és hangfelvétel védelmét más szempontok szerint más jogterületek is biztosítják, különösen a személyes adat védelmét szolgáló adatvédelmi jog. A védelem párhuzamos jellege az oltalmazott értékek becses voltát hangsúlyozza.” A Ptk. által meghatározott „hozzájárulás” nem azonos az adatkezelés jogalapjával, mely a jogszerű adatkezelés elengedhetetlen feltétele, és melyről a GDPR és az Infotv rendelkezik. A más képmásával, hangfelvételével kapcsolatos bármilyen jogosulatlan, beavatkozó magatartás jogsértő. A védelem objektív jellegű. Mindenkinek alanyi joga eldönteni, hogy kívánja-e, hogy róla vagy hangjáról felvétel készüljön, és kívánja-e, hogy az bármilyen nyilvánosság elé kerüljön, hozzájárul-e ahhoz. A jog ugyanakkor a képmáshoz való jogot is a feltétlenül szükséges mértékben, az elérni kívánt céllal arányosan, a jog lényeges tartalmának tiszteletben tartásával korlátozza; a Kfttv. közbiztonsági, bűnmegelőzési célból lehetővé teszi, hogy közterületen, bárki számára észlelhető módon, előzetes tájékoztatási kötelezettséggel egyetemben képfelvevő kerüljön elhelyezésre.

c) elérni kívánt célmeghatározása	Az adatkezelés jelentősen nem korlátozza az érintettek magánszféráját, adatkezelő a felvételeket kizárólag az esetleges jogsértések, szabálysértések, bűncselekmények elkövetése esetén használja fel, a Kttfv-nek megfelelően továbbítja a hatáskörrel és illetékességgel rendelkező hatóságoknak.
d) annak leírása, hogy az adatkezelés miért hatékony és miért a legkevésbé korlátozó eszköz a cél eléréséhez	Az adatkezelés célját törvény határozza meg; Magyarország helyi önkormányzatairól szóló 2011. évi CLXXXIX. törvény (Mötv.) 13. § (1) bekezdés 17. pontjában meghatározott, a helyi közügyek, valamint a helyben biztosítható közfeladatok körében ellátandó, Teresztenye település közbiztonságában való közreműködés mint helyi önkormányzati feladat ellátása. Adatkezelő Teresztenye Község Önkormányzata e feladatkörében eljárva, a közterület-felügyeletről szóló 1999. évi LXIII. törvény (Kttfv.) 7. § (3) bekezdése szerint a közterületen közbiztonsági, illetve bűnmegelőzési célból döntött a bárki számára nyilvánvalóan észlelhető módon történő képfelvévők elhelyezéséről. Teresztenye 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.
V. Érintetti érdekek, biztosítékok	A közbiztonság, bűnmegelőzési cél és a település lakosainak biztonságérzetének javítása hatékonyan elérhető közterületi képfelvévők elhelyezésével. Élőkép megfigyelése nem történik, a képfelvételek kizárólag a Kttfv-ben foglalt esetekben kerülnek megtekintésre, indokolt esetben továbbításra.
8. Érintett jogainak, érdekeinek beazonosítása	A személyes adatok védelmét és a képmáshoz való jogot adatkezelő jelen érdekmérlegelésben azonosította. Az érintett érdeke a tulajdon sértetlensége, javainak védelme, az esetleges károk megtérítése.
9. Érintett észszerű elvárásai	Az érintett észszerű elvárásai között szerepelhet, hogy képmását cél nélkül, vagy a jelen érdekmérlegelésben meghatározott célon kívüli célokra ne használja adatkezelő, a személyes adatok kezelésére a lehető legrovidebb kerülijön sor, a személyes adatait a lehető legszűkebb személyi kör ismerhesse meg. Ésszerű elvárás továbbá, hogy az adatkezelésről előzetes tájékoztatást kapjon, továbbá rejtett kamerás megfigyelésre és a magánterülete megfigyelésére ne kerüljön sor.
10. Érintettre gyakorolt hatás	Az adatkezelés az érintett információs önrendelkezési jogára van hatással, tekintettel arra, hogy a személyes adatok kezelésére az érintett hozzájárulása nélkül kerül sor.
VI. Szembenálló érdekek mérlegelése	
11. Arányosság bemutatása	
a) érintetti kör	Település lakosai, továbbá azon személyek, akik a település kamerával megfigyelt területeire belépnek.
b) személyes meghatározása/adatkategóriák	Képmás, gépjármű típusa, forgalmi rendszám. Személyes adatnak is minősülő képfelvételek kerülnek rögzítésre, tárolásra, a felvételen beazonosítható természetes személyek jelenhetnek meg különböző mozgást, magatartást megvalósítva, amelyből akár közvetlen vagy közvetlen következtetések is levonhatók.
c) milyen forrásból gyűjtik az adatokat	A személyes adatok az érintettől származnak.

d) adatkezelés időtartama	A képfeltevő eszközzel rögzített videofelvételek megőrzési ideje a Kfttv. 7. § (7) bekezdés b) pontja szerint a rögzítést követő 30 nap.
e) érintettek számíthatnak-e a hozzájárulásuk nélküli adatkezelésre	Az adatkezelést megelőzően adatkezelő kikérte a település lakosainak véleményét a tervezett adatkezelésről, melyet adatkezelő dokumentált. Az adatkezelést a település lakosai igényelték. Tekintettel arra, hogy az adatkezelésre közbiztonsági, bűnmegelőzési célokból törvényi felhatalmazás alapján joga van valamennyi önkormányzatnak, a Mőtv. 13. § (1) bekezdés 17. pontja alapján az önkormányzatoknak felelősséget kell vállalniuk a bűnözés visszaszorításában, az adatkezelő megítélése szerint az adatkezelésre az érintettek számíthatnak. Az érintettek megfelelő tájékoztatását elősegíti a jól látható helyen elhelyezett kamerák, valamint a kamerás megfigyelésre figyelemzettető táblák, illetőleg a település honlapján elérhető tájékoztató.
f) érintettet érő kedvező és kedvezőtlen hatások	Az adatkezelő és az érintett érdekei többnyire egybeesnek. A közterületen történtek rögzítése a közbiztonság, bűnmegelőzés céljából a lakosság biztonságérzetének növelését eredményezi. A kamerák elhelyezése, a beállított látószögek alkalmazása az esetlegesen jogellenes cselekmények felderítésére, és akár kártérítési igény megalapozására. Azon érintettek nézve, akik elhaladnak a kamerák által megfigyelt területeken, kedvezőtlen hatással lehet a felvétel készítése, figyelemmel arra, hogy a képfelvételre nem hozzájárulás alapján kerül sor, azonban adatkezelőnek nem célja a szisztematikus megfigyelés, élőképfelvétele sem történik, ezért ezen hatás elhanyagolható az adatkezelési cél megvalósulása szempontjából.
g) érintetti joggyakorlás lehetősége	A Kfttv. 7. § (4)-(5) bekezdése alapján adatkezelő a képfeltevők elhelyezéséről és a képfeltevők által megfigyelt közterületről az önkormányzat honlapján tájékoztatást ad, az információkat közzéteszi. Adatkezelő a képfeltevő által megfigyelt területre belépő személyek tájékoztatását elősegítő módon figyelemfelhívó jelzést, ismertetést helyez el a képfeltevők elhelyezéséről, az adatkezelés tényéről a lakott terület kezdetét jelző táblánál és a képfeltevők elhelyezését biztosító oszlopokon (elsődleges tájékoztatás). Adatkezelő a részletes adatkezelési tájékoztatót Teresztenye Község Önkormányzatának honlapján közzéteszi, valamint Teresztenye Község Önkormányzatának hivatali épületében is megtekinthető (3757 Teresztenye Rákóczi Ferenc út 18.).
12. Garanciák (idő, hozzáférés, egyéb adatbiztonsági intézkedések)	Az adatkezelésre törvény felhatalmazása alapján kerül sor, mely adatkezelés szükségességéről képviselő-testületi döntés született, a településen élők előzetes véleménynyilvánítását is figyelembe véve. A rögzített kamerafelvételekhez kizárólag a képviselő-testület által kijelölt személy, valamint a képviselő-testület által elfogadott adatfeldolgozó az adatfeldolgozási szerződés keretein belül fér hozzá. A kamerás megfigyelésre adatkezelő szabályzatot fogadott el. A kamerafelvételek visszanézésére a szabályzatban foglaltak az irányadóak.

13. Adatkezelés bemutatása	hasznosságának	Az adatkezelés Teresztenye településen a közrend, közbiztonság, bűnmegelőzés céljából, a településen élők biztonságérzetének növelése érdekében hasznos, az adatkezelés mind az adatkezelő, mind a település lakosai mint érintettek érdekében áll. Adatkezelő Teresztenye Község Önkormányzata Borsod-Abaúj-Zemplén vármegyében található zsáktelepülés. A rendőrség hivatalos adatai szerint a vármegyében regisztrált bűncselekmények száma az országos átlaghoz képest magas, ezért kiemelten fontos a közbiztonság, bűnmegelőzés szerepe, melyben a Mötv. 13. § (1) bekezdés 17. pontja alapján az önkormányzatoknak is felelősséget kell vállalniuk. A településen főleg időskorúak élnek, a 60 év felettiek aránya kb. 70-80%.
VII. Eredmény		
14. Szükséges és arányosság eldöntése		A megfigyelt területre belépő természetes személyek alapvető jogait és szabadságát az adatkezelés jelentős mértékben nem, az adatkezelés kockázatainak mérséklése érdekében tett adatkezelői intézkedések miatt elhanyagolható mértékben korlátozza, az érintettek jogai nem élveznek elsőbbséget az adatkezelő jogos érdekével szemben, az adatkezelés szükséges és arányos.

Lenyeges következmények

érintett napi rutinjának me.
személyes adattal visszaélés
jóhírnév sértése
Az adatok más célokból történő felhasználása
bíróági, hatósági eljárásb...
utólagos módosítással nem
érintetti joggyakorlás nem

Fenyegető veszély

Szervezeten kívüli rosszhis
Szervezeten belüli rosszhis
Szervezeten belüli rosszhis
nem emberi tényezők (pl. id
emberi tényező: rosszhisze
tűz, természeti csapás
Szervezeten belüli rosszhis
Szervezeten kívüli rosszhis

Források

Szervezeten belüli: adatkeze
Szervezeten kívüli: fogadó
Nem emberi tényezők: tűz
nem emberi tényezők (pl. id
emberi tényezők: rosszhisze
Szervezeten belüli: jogosul
Szervezeten kívüli: jogosul
Tűz vagy természeti csapás

Intézkedések

Logikai hozzáférés szabály
Szabályzatok
Adatfeldolgozók igénybevé
Nyomon követhetőség (nap
Humánerőforrás-menedzsm
Szervezet
Az adatvédelem beépítése a
Fizikai hozzáférésvédelem
Hálózatbiztonság
Adatvédelmi kockázatok ke
Adatminimalizálás
A munkaállomások kezelés
Kapcsolat harmadik felekke
Hardwarebiztonság
Karbantartás
Papír alapú dokumentumok

Az adatokhoz való jogosulatlan hozzáférés

Súlyosság : Korlátozott

Valószínűség : Elhanyagolható

Az adatok véletlen vagy jogellenes megváltoztatása

Súlyosság : Elhanyagolható

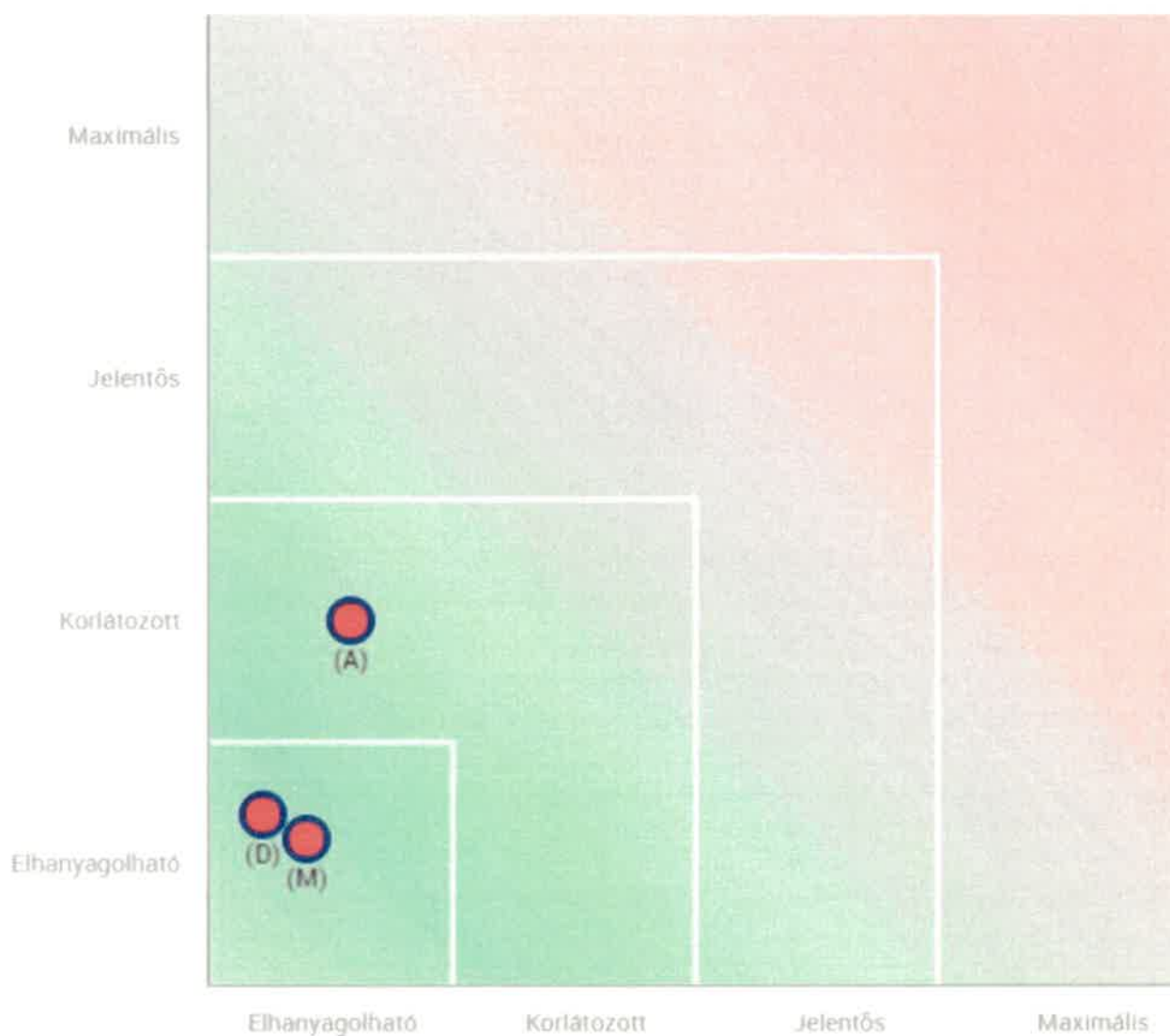
Valószínűség : Elhanyagolható

Adatvesztés

Súlyosság : Elhanyagolható

Valószínűség : Elhanyagolható

Kockázat súlyossága



- **Tervezett vagy meglévő intézkedések figyelembevételével**
- **A** korrekciós intézkedéseket is tekintetbe véve
- (A) Adatokhoz való jogosulatlan hozzáférés
- (M) Az adatok véletlen vagy jogellenes megváltoztatása
- (D) Adatvesztés

Kockázat valószínűsége

Áttekintés

Alapelvek		Tervezett vagy meglévő intézkedések	
Célok			Logikai hozzáférés szabályozás
Jogalap			Nyomon követhetőség (naplózás)
Megfelelő adatok			Szabályzatok
Pontosság			Humánerőforrás-menedzsment
Adatmegőrzési határidő			Karbantartás
Az érintettek tájékoztatása			Adatfeldolgozók igénybevétele során alkalmazandó követelmények
A hozzájárulás megszerzése			Hálózatbiztonság
Az érintettek tájékoztatása			Fizikai hozzáférésvédelem
A helyesbítéshez és a törléshez való jog			Szervezet
Az adatkezelés korlátozáshoz és a tiltakozáshoz való jog			Adatvédelmi kockázatok kezelése
Adatfeldolgozók igénybevétele			Az adatvédelem beépítése a projektekbe
Adattovábbítások			Papír alapú dokumentumok biztonsága
			Adatminimalizálás
			A munkaadómások kezelése
			Kapcsolat harmadik felekkel
			Hardwarebiztonság
		Kockázatok	
			Adatokhoz való jogosulatlan hozzáférés
			Az adatok véletlen vagy jogellenes megváltoztatása
			Adatvesztés

Korrektíós Intézkedések

Elfogadható Intézkedések

Térfigyelő kamerarendszerrel kapcsolatos adatkezelési tájékoztató

2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról alapján

Adatkezelő neve: Teresztenye Község Önkormányzata
Címe (hivatalos levelezési cím): 3757 Teresztenye, Rákóczi Ferenc út 18
E-mail cím: teresztenyefonix@gmail.com
Honlapjának elérhetősége:
Telefonszáma: +36 48 463502
Adószáma: 15547633-1-05
Cégjegyzékszám, nyilvántartási szám: 547633
Képviselője neve: Brogli Attila
Adatvédelmi tisztviselő / felelős neve: GDPR Reg Kft.
Adatvédelmi tisztviselő / felelős elérhetősége: adatvedelem@teresztenye.hu
Adatkezelési tájékoztató elérhetősége: <https://teresztenye.asp.lgov.hu/>

Adatkezelő fenntartja a jogot, hogy a jelen Tájékoztatót egyoldalúan, a módosítást követő hatállyal módosítsa. Erre tekintettel ajánlott rendszeresen látogatni weboldalát abból a célból, hogy figyelemmel kísérhesse a változásokat. Kérésére a módosításokról értesítést küldünk, vagy megküldjük a mindenkor hatályos Tájékoztató egy példányát.

A kezelt adatok köre és adatkezelési célok

Az adatkezelés az Infotv. rendelkezéseinek megfelelően történik.

Tájékoztatjuk, hogy jogszabály felhatalmazása alapján más szervek (pl.: bíróság, ügyész, nyomozó hatóság, szabálysértési hatóság, közigazgatási hatóság, Nemzeti Adatvédelmi és Információszabadság Hatóság) tájékoztatás adása, adatok közlése, átadása, iratok rendelkezésre bocsátása végett megkereshetik Adatkezelőt. Ha a hatóság a pontos célt és az adatok körét megjelölte, személyes adatot csak annyit és olyan mértékben adunk ki, amely a megkeresés céljának megvalósításához elengedő és amire a jogszabályi felhatalmazás alapot ad.

E tájékoztatóban fel nem sorolt adatkezelésekről az adat felvételekor adunk tájékoztatást.

Az adatkezelés célja: Települési térfigyelő kamerarendszer

Adatkezelés leírása: A térfigyelő rendszer üzemeltetés célja a település közbiztonságának növelése, bűnmegelőzés, a jogellenes köztéri magatartások megelőzése és felderítésük elősegítése, a közterületi rendre vonatkozó előírások betartásának ellenőrzése, az önkormányzati vagyon védelme. 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. Amennyiben a kamerarendszer által rögzített adatok felhasználásra kerülnek, akkor személyes adatnak tekinthető az érintett magatartása is mint az érintettre vonatkozó következtetés. A rögzített képfelvétel felhasználás hiányában a rögzítéstől számított 30 nap elteltével törlésre kerül. Felhasználásnak az minősül, ha a rögzített felvételt bírósági vagy más hatósági eljárásban bizonyítékként felhasználják. Az adatkezelés részleteit, az egyes kamerák elhelyezését, látószögét külön szabályzat (Közterületi térfigyelő kamerarendszer adatvédelmi szabályzat) tartalmazza. A képfelvételek elhelyezésére, a megfigyelt területre vonatkozó adatok, a kamerák pontos helyszíne, elhelyezése a település honlapján is megtekinthető.

Az adatkezelés jogalapja: 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról, 5. § (1) a), Magyarország helyi önkormányzatairól szóló 2011. évi CLXXXIX. törvény 13. § (1) 17. pont, 17. §, 1999. évi LXIII. törvény a közterület-felügyeletről 1. §, 7. § (3), 8. § (1)

Vonatkozó jogszabály(ok): Az adatkezelés jogalapja: 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról, 5. § (1) bek. a) pont - azt törvény vagy - törvény felhatalmazása alapján, az abban meghatározott körben, különleges adatnak vagy bűnügyi személyes adatnak nem minősülő adat esetén - helyi önkormányzat rendelete közérdeken alapuló célból elrendeli, ill. a település közterületei biztonságának és jogszertű használatának biztosítása a Magyarország helyi önkormányzatairól szóló 2011. évi CLXXXIX. törvény 13. § (1) bek. 17. pont, 17. §, 1999. évi LXIII. törvény a közterület-felügyeletről 1. §, 7. § (3) bek., 8. § (1) bek.

Adatszolgáltatás elmaradásának lehetséges következményei: Közérdekből vagy közhatalom gyakorlásához szükséges adatkezelés. Közbiztonsági, bűnmegelőzési cél nem teljesül.

Érintettek: Közterületi kamerák látóterében megjelenő személy

Adatok forrása: Érintett

Adatkezelés tervezett időtartamának alapja: Az adatkezelés kezdete

A kezelt adatok köre, időtartama: Érintett képmása, mozgása, ehhez köthető azonosító adatok, rendszám: 30 nap

Harmadik országba történő adattovábbítás garanciái: Nem történik harmadik országba adattovábbítás

Térfigyelő kamerarendszerrel kapcsolatos adatkezelési tájékoztató

2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról alapján

Adatfeldolgozó: Közterületi kamerarendszer karbantartása: BORSODWEB Internet Szolgáltató Kft. (3527 Miskolc, József Attila utca 27. II. em. 1. ajtó)

Címzettek: A közterületi kamerák által készített kép és videofelvételek a Kftv. 7.§ (6) bekezdésében foglalt felhasználási célokból a szabálysértési eljárásra jogosult szerv, büntetőeljárásban a bíróság, az ügyészség, a nyomozó hatóság, az előkészítő eljárást folytató szerv részére, illetve a Kftv. 7. § (6a) bekezdésében meghatározott célból a nemzetbiztonsági szolgálat, a hivatásos katasztrófavédelmi szerv és a közigazgatási hatósági eljárást lefolytató szerv részére kerülhetnek továbbításra. A felvételek továbbításáról az adatkezelő nyilvántartást vezet.

Az érintett jogai

Érintett jogosult arra, hogy törvényben meghatározott jogainak érvényesítése érdekében Adatkezelőhöz forduljon.

Adatkezelő az érintett jogai gyakorlására irányuló kérelmét az annak beérkezésétől számított legfeljebb huszonöt napon belül elbírálja és döntéséről az érintettet írásban vagy elektronikus úton értesíti. A kérelem beérkezésének napja a határidőbe nem számít bele.

Az Infotv-nek megfelelően az érintettek az alábbi főbb jogokat gyakorolhatják:

a. Az előzetes tájékozódáshoz való jog:

Az érintett jogosult arra, hogy a Adatkezelő által kezelt, személyes adatai vonatkozásában az adatkezelést megelőzően tájékoztatást kapjon az adatkezeléssel kapcsolatos alábbi tényekről: az adatkezelő, illetve adatfeldolgozó megnevezése és elérhetősége; az adatvédelmi tisztviselő neve és elérhetősége; az adatkezelés célja; az adatkezelés jogalapja; a kezelt személyes adatok megőrzésének időtartama; az adattovábbítás címzettjei; a kezelt személyes adatok gyűjtésének forrásai; az érintettet az Infotv. alapján megillető jogok, valamint azok érvényesítésének módja.

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

Adatkezelő a képfelvevők 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

b. Hozzáféréshez való jog:

Az érintett jogosult arra, hogy kérelmére személyes adatait és azok kezelésével összefüggő információkat Adatkezelő a rendelkezésére bocsássa, így különösen: az adatkezelést maga az adatkezelő, illetve megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó végzi-e, a kezelt személyes adatok forrását, az adatkezelés célját és jogalapját, a kezelt személyes adatok körét, a kezelt személyes adatok továbbítása esetén az adattovábbítás címzettjeinek - ideértve a harmadik országbeli címzetteket és nemzetközi szervezeteket - körét, a kezelt személyes adatok megőrzésének időtartamát, ezen időtartam meghatározásának szempontjait, az érintettet az Infotv. alapján megillető jogok, valamint azok érvényesítése módjának ismertetését, profilalkotás alkalmazásának esetén annak tényét és az érintett személyes adatainak kezelésével összefüggésben felmerült adatvédelmi incidensek bekövetkezésének körülményeit, azok hatásait és az azok kezelésére tett intézkedéseket.

c. Helyesbítéshez való jog:

Az érintett jogosult arra, hogy kérelmére Adatkezelő vagy megbízásából adatfeldolgozó által kezelt személyes adatokat Adatkezelő haladéktalanul pontosítsa, helyesbítse, illetőleg, ha az adatkezelés céljával összeegyeztethető, kiegészítse akkor, ha a kezelt személyes adatok pontatlanok, helytelenek vagy hiányosak.

Adatkezelő mentesül a fenti kötelezettség alól, ha a pontos, helytálló, illetve hiánytalan személyes adatok nem állnak rendelkezésére és azokat az érintett sem bocsátja a rendelkezésére, vagy az érintett által rendelkezésére bocsátott személyes adatok valóságára kétséget kizáróan nem állapítható meg.

A helyesbítéshez való jog nem gyakorolható a felvételeken szereplő személyes adatok vonatkozásában.

d. Az adatkezelés korlátozásához való jog:

Adatkezelő köteles az érintett kérelmére vagy az Infotv. 19. §-ában meghatározott esetekben az érintett személyes adatai kezelésének korlátozására. Az adatkezelés korlátozásának időtartama alatt a korlátozással érintett személyes adatokkal Adatkezelő a tároláson túl egyéb adatkezelési műveletet kizárólag az érintett jogos érdekének érvényesítése

Térfigyelő kamerarendszerrel kapcsolatos adatkezelési tájékoztató

2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról alapján

céljából vagy törvényben, nemzetközi szerződésben, illetve az Európai Unió kötelező jogi aktusában meghatározottak szerint végezhet.

e. Törléshez való jog:

Adatkezelő az érintett kérelmére, valamint az Infotv. 20. §-a szerint, az alább meghatározott esetekben törli az érintett személyes adatait.

Adatkezelő haladéktalanul törli az érintett személyes adatait, ha az adatkezelés jogellenes, az érintett az adatkezeléshez adott hozzájárulását visszavonja vagy a személyes adatainak törlését kéri (kivéve, ha az adatkezelést törvény vagy helyi önkormányzat rendelete közérdeken alapuló célból rendeli el, illetve az adatkezelés az érintett vagy más személy létfontosságú érdekeinek védelméhez, valamint a személyek életét, testi épségét vagy javait fenyegető közvetlen veszély elhárításához vagy megelőzéséhez szükséges és azzal arányos, különleges adat esetén ha az törvényben kihirdetett nemzetközi szerződés végrehajtásához feltétlenül szükséges és azzal arányos, vagy azt az Alaptörvényben biztosított alapvető jog érvényesítése, továbbá a nemzetbiztonság, a bűncselekmények megelőzése, felderítése vagy üldözése érdekében vagy honvédelmi érdekből törvény elrendeli), az adatok törlését jogszabály, az Európai Unió jogi aktusa, a Nemzeti Adatvédelmi és Információszabadság Hatóság (Hatóság) vagy a Bíróság rendelte el, továbbá az Infotv. 19. § (1) bekezdés b)-d) pontjában meghatározott időtartam eltelt.

f. Jogorvoslathoz/panasztételhez való jog

Amennyiben Adatkezelő által folytatott adatkezeléssel kapcsolatban kérdése, panasza merül fel, vagy az előzőekben ismertetett jogait kívánja gyakorolni, úgy az érintett közvetlenül fordulhat Adatkezelőhöz, vagy az adatvédelmi tisztviselőjéhez a jelen tájékoztatóban megadott elérhetőségeken.

Az érintett kezdeményezheti a Hatóság vizsgálatát az adatkezelői intézkedések jogszerűségének vizsgálata céljából, ha Adatkezelő az érintett előzőekben felsorolt jogainak érvényesítését korlátozza vagy a kérelmét elutasítja; továbbá a Hatóság adatvédelmi hatósági eljárásának lefolytatását kérelmezheti, amennyiben megítélése szerint Adatkezelő a személyes adatainak kezelése során megsértette a személyes adatok kezelésére vonatkozó jogszabályi előírásokat.

Az érintett Adatkezelő – illetve az adatfeldolgozó tevékenységi körébe tartozó adatkezelési műveletekkel összefüggésben – az adatfeldolgozó ellen bírósághoz fordulhat, ha megítélése szerint az adatkezelő, illetve az általa megbízott vagy rendelkezése alapján eljáró adatfeldolgozó a személyes adatok kezelésére vonatkozó, jogszabályban vagy az Európai Unió kötelező jogi aktusában meghatározott előírások megsértésével kezeli. A pert az érintett - választása szerint - a lakóhelye vagy tartózkodási helye szerint illetékes törvényszék előtt is megindíthatja. Az illetékes törvényszéket megkeresheti a <https://birosag.hu/birosag-kereso> weboldalon.

A Nemzeti Adatvédelmi és Információszabadság Hatóság elérhetőségei:

1055 Budapest, Falk Miksa utca 9-11., Postacím: 1363 Budapest, Pf. 9.
Telefonszám: +36 1 391 1400; fax: +36 1 391 1410;
e-mail: ugyfelszolgalat@naih.hu; honlap: www.naih.hu

