FONYÓDI VÁROSFEJLESZTÉSI ÉS VÁROSÜZEMELTETÉSI NONPROFIT KÖZHASZNÚ KFT.

ADATVÉDELMI SZABÁLYZAT

Hatálybalépés dátuma:2018. május 24.

Tartalomjegyzék

A Fonyódi Városfejlesztési és Városüzemeltetési Nonprofit Közhasznú Kft. (a továbbiakban: Társaság vagy Adatkezelő) belső adatkezelési folyamatainak nyilvántartása és az érintettek jogainak biztosítása céljából az alábbi Adatvédelmi és Adatbiztonsági Szabályzatot alkotja.

Adatkezelő megnevezése:	Fonyódi Városfejlesztési és Városüzemeltetési Nonprofit Közhasznú Kft.
Adatkezelő cégjegyzékszáma:	14-09-312254
Adatkezelő székhelye:	8640 Fonyód, Vágóhíd u. 17.
Adatkezelő honlapjának címe:	www.fonyodert.hu
Adatkezelő e-mail címe:	info@fonyodert.hu
Adatkezelő képviselője:	Kristóf Györgyné ügyvezető igazgató
Adatkezelő telefonszáma:	+36 85 560 287

Jelen rendelkezéseket a Társaság többi szabályzatának előírásaival összhangban kell értelmezni. Amennyiben a személyes adatok védelmével kapcsolatosan ellentmondás áll fent jelen rendelkezések és a bármely más, jelen szabályzat hatálybalépése előtt hatályba lépett szabályzat előírásai között, úgy abban az esetben jelen rendelkezések az irányadóak.

1. A SZABÁLYZAT CÉLJA ÉS HATÁLYA

A Társaság jelen szabályzat megalkotásával és elérhetővé tételével biztosítani kívánja az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) 15. §-ában meghatározott érintetti tájékoztatáshoz való jog megvalósulását.

Jelen szabályzat célja, hogy az érintettek megfelelő tájékoztatást kaphassanak a Társaság által kezelt, illetve az általa megbízott adatfeldolgozó által feldolgozott adatokról, azok forrásáról, az adatkezelés céljáról, jogalapjáról, időtartamáról, az adatkezelésbe esetlegesen bevont adatfeldolgozó nevéről, címéről és az adatkezeléssel összefüggő tevékenységéről, továbbá - az érintett személyes adatainak továbbítása esetén - az adattovábbítás jogalapjáról és címzettjéről.

Jelen szabályzattal a Társaság biztosítani kívánja a nyilvántartások működésének törvényes rendjét, az adatvédelem alkotmányos elveinek, az adatbiztonság követelményeinek érvényesülését, meg kívánja akadályozni az adatokhoz való jogosulatlan hozzáférést, és azok jogosulatlan megváltoztatását, illetve nyilvánosságra hozatalát.

A szabályzat tárgyi hatálya kiterjed a Társaság minden szervezeti egységénél folytatott valamennyi olyan folyamatra, amely során az Infotv. 3. § 2. pontjában meghatározott személyes adat kezelése megvalósul.

2. FOGALMAK

A jelen szabályzat fogalmi rendszere megegyezik az Infotv.-ben és az Európa Parlament és a Tanács (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 rendelet hatályon kívül helyezéséről szóló rendeletben (a továbbiakban: GDPR, vagy Rendelet) meghatározott értelmező fogalommagyarázatokkal, így különösen:

- **Érintett:** bármely meghatározott, személyes adat alapján azonosított vagy – közvetlenül vagy közvetve - azonosítható természetes személy;
- **Személyes adat**: az érintettel kapcsolatba hozható adat - különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret -, valamint az adatból levonható, az érintettre vonatkozó következtetés;
- **Különleges adat:**
  - a faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdekképviseleti szervezeti tagságra, a
  - szexuális életre vonatkozó személyes adat,
  - az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat, valamint a bűnügyi személyes adat;
- **Bűnügyi személyes adat:** a büntetőeljárás során vagy azt megelőzően a bűncselekménnyel vagy a büntetőeljárással összefüggésben, a büntetőeljárás lefolytatására, illetve a bűncselekmények felderítésére jogosult szerveknél, továbbá a büntetés-végrehajtás szervezeténél keletkezett, az érintettel kapcsolatba hozható, valamint a büntetett előéletre vonatkozó személyes adat;
- **Hozzájárulás:** az érintett akaratának önkéntes és határozott kinyilvánítása, amely megfelelő tájékoztatáson alapul, amellyel félreérthetetlen beleegyezését adja a rá vonatkozó személyes adat
  - teljes körű vagy egyes műveletekre kiterjedő - kezeléséhez;
- **Tiltakozás:** az érintett nyilatkozata, amellyel személyes adatának kezelését kifogásolja és az adatkezelés megszüntetését, illetve a kezelt adat törlését kéri;
- **Adatkezelő:** az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely önállóan vagy másokkal együtt az adat kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja;
- **Adatkezelés:** az alkalmazott eljárástól függetlenül az adaton végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, továbbá az adat további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése;
- **Adattovábbítás:** az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele;
- **Nyilvánosságra hozatal:** az adat bárki számára történő hozzáférhetővé tétele;
- **Adattörlés:** az adat felismerhetetlenné tétele oly módon, hogy a helyreállítása többé nem lehetséges;
- **Adatzárolás:** az adat azonosító jelzéssel ellátása további kezelésének végleges vagy meghatározott időre történő korlátozása céljából;

- **Adatmegjelölés:** az adat azonosító jelzéssel ellátása annak megkülönböztetése céljából;
- **Adatmegsemmisítés:** az adatot tartalmazó adathordozó teljes fizikai megsemmisítése;
- **Adatfeldolgozás:** az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől, feltéve, hogy a technikai feladatot az adaton végzik;
- **Adatfeldolgozó:** az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely szerződés alapján - beleértve a jogszabály rendelkezése alapján kötött szerződést is - adatok feldolgozását végzi;
- **Adatállomány:** az egy nyilvántartásban kezelt adatok összessége;
- **Harmadik személy:** olyan természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely nem azonos az érintettel, az adatkezelővel vagy az adatfeldolgozóval;
- **EGT-állam:** az Európai Unió tagállama és az Európai Gazdasági Térségről szóló megállapodásban részes más állam, továbbá az az állam, amelynek állampolgára az Európai Unió és tagállamai, valamint az Európai Gazdasági Térségről szóló megállapodásban nem részes állam között létrejött nemzetközi szerződés alapján az Európai Gazdasági Térségről szóló megállapodásban részes állam állampolgárával azonos jogállást élvez;
- **Harmadik ország:** minden olyan állam, amely nem EGT-állam;
- **Adatvédelmi incidens:** személyes adat jogellenes kezelése vagy feldolgozása, így különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés;
- **Adatkezelés korlátozása:** a tárolt személyes adatok megjelölése jövőbeli kezelésük korlátozása céljából;
- **Álnevesítés:** a személyes adatok olyan módon történő kezelése, amelynek következtében további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik, feltéve, hogy az ilyen további információt külön tárolják, technikai és szervezési intézkedések megtételével biztosított, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet kapcsolni;
- **Biometrikus adat:** egy természetes személy testi, fiziológiai vagy viselkedési jellemzőire vonatkozó minden olyan sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását, ilyen például az arckép vagy a daktiloszkópiai adat;
- **Címzett:** az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, akivel vagy amellyel a személyes adatot közlik, függetlenül attól, hogy harmadik fél-e. Azon közhatalmi szervek, amelyek egy egyedi vizsgálat keretében az uniós vagy a tagállami joggal összhangban férhetnek hozzá személyes adatokhoz, nem minősülnek címzettnek; az említett adatok e közhatalmi szervek általi kezelése meg kell, hogy feleljen az adatkezelés céljainak megfelelően az alkalmazandó adatvédelmi szabályoknak;
- **Egészségügyi adat:** egy természetes személy testi vagy pszichikai egészségi állapotára vonatkozó személyes adat, ideértve a természetes személy számára nyújtott egészségügyi szolgáltatásokra vonatkozó olyan adatot is, amely információt hordoz a természetes személy egészségi állapotáról;
- **Harmadik fél:** az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely nem azonos az érintettel, az adatkezelővel, az adatfeldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére felhatalmazást kaptak;
- **Genetikai adat:** egy természetes személy örökölt vagy szerzett genetikai jellemzőire vonatkozó minden olyan személyes adat, amely az adott személy fiziológiájára vagy egészségi állapotára vonatkozó egyedi információt hordoz és amely elsősorban az említett természetes személyből vett biológiai minta elemzéséből ered;

- **Képviselő:** az az Unióban tevékenységi hellyel, illetve lakóhellyel rendelkező és az adatkezelő vagy adatfeldolgozó által írásban megjelölt természetes vagy jogi személy, aki, illetve amely az adatkezelőt vagy adatfeldolgozót képviseli az adatkezelőre vagy adatfeldolgozóra az a Rendelet értelmében háruló kötelezettségek vonatkozásában;
- **Kötelező erejű vállalati szabályok:** a személyes adatok védelmére vonatkozó szabályzat, amelyet az Unió valamely tagállamának területén tevékenységi hellyel rendelkező adatkezelő vagy adatfeldolgozó egy vagy több harmadik országban a személyes adatoknak az ugyanazon vállalkozáscsoporton vagy közös gazdasági tevékenységet folytató vállalkozások ugyanazon csoportján belüli adatkezelő vagy adatfeldolgozó részéről történő továbbítása vagy ilyen továbbítások sorozata tekintetében követ;
- **Nyilvántartási rendszer:** a személyes adatok bármely módon – centralizált, decentralizált, funkcionális vagy földrajzi szempontok szerint – tagolt állománya, amely meghatározott ismérvek alapján hozzáférhető;
- **Profilalkotás:** személyes adatok automatizált kezelésének bármely olyan formája, amelynek során a személyes adatokat valamely természetes személyhez fűződő bizonyos személyes jellemzők értékelésére, különösen a munkahelyi teljesítményhez, gazdasági helyzethez, egészségi állapothoz, személyes preferenciákhoz, érdeklődéshez, megbízhatósághoz, viselkedéshez, tartózkodási helyhez vagy mozgáshoz kapcsolódó jellemzők elemzésére, illetve előrejelzésére használják;
- **Releváns és megalapozott kifogás:** a döntéstervezettel szemben benyújtott, azzal kapcsolatos kifogás, hogy a Rendeletet megsértették-e, illetve, hogy az adatkezelőre vagy az adatfeldolgozóra vonatkozó tervezett intézkedés összhangban van-e a Rendelettel; a kifogásban egyértelműen be kell mutatni a döntéstervezet által az érintettek alapvető jogaira és szabadságaira, valamint adott esetben a személyes adatok Unión belüli szabad áramlására jelentett kockázatok jelentőségét;
- **Tevékenységi központ:**
  a) az egynél több tagállamban tevékenységi hellyel rendelkező adatkezelő esetében az Unión belüli központi ügyvitelének helye, ha azonban a személyes adatok kezelésének céljaira, valamint eszközeire vonatkozó döntéseket az adatkezelő egy Unión belüli másik tevékenységi helyén hozzák és az utóbbi tevékenységi hely rendelkezik hatáskörrel az említett döntések végrehajtatására, az említett döntéseket meghozó tevékenységi helyet kell tevékenységi központnak tekinteni;
  b) az egynél több tagállamban tevékenységi hellyel rendelkező adatfeldolgozó esetében az Unión belüli központi ügyvitelének helye, vagy ha az adatfeldolgozó az Unióban nem rendelkezik központi ügyviteli hellyel, akkor az adatfeldolgozónak az az Unión belüli tevékenységi helye, ahol az adatfeldolgozó tevékenységi helyén folytatott tevékenységekkel összefüggésben végzett fő adatkezelési tevékenységek zajlanak, amennyiben az adatfeldolgozóra a Rendelet szerint meghatározott kötelezettségek vonatkoznak;
- **Vállalkozás:** gazdasági tevékenységet folytató természetes vagy jogi személy, függetlenül a jogi formájától, ideértve a rendszeres gazdasági tevékenységet folytató személyegyesítő társaságokat és egyesületeket is;
- **Vállalkozáscsoport:** az ellenőrző vállalkozás és az általa ellenőrzött vállalkozások;

Amennyiben a mindenkori hatályos adatvédelmi jogszabály (jelen szabályzat megalkotásakor az Infotv. és a GDPR) fogalommagyarázatai eltérnek jelen szabályzat fogalommagyarázataitól, akkor a jogszabály által meghatározott fogalmak az irányadók.

3. AZ ADATKEZELÉSEK SZABÁLYAI

Mivel az információs önrendelkezés minden természetes személy Alaptörvényben rögzített alapjoga, így a Társaság eljárásai során csak és kizárólag a hatályos jogszabályok rendelkezései alapján végez adatkezelést.

Személyes adat kezelésére csak jog gyakorlása vagy kötelezettség teljesítése érdekében van lehetőség. A Társaság által kezelt személyes adatok magáncélra való felhasználása tilos. Az adatkezelésnek mindenkor meg kell felelnie a célhoz kötöttség alapelvének.

A Társaság személyes adatot csak meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében kezel, a cél eléréséhez szükséges minimális mértékben és ideig. Az adatkezelés minden szakaszában meg kell felelnie a célnak – amennyiben az adatkezelés célja megszűnt, vagy az adatok kezelése egyébként jogellenes, az adatok törlésre kerülnek. A törlésről a Társaságnak az adatot ténylegesen kezelő munkavállalója gondoskodik. A törlést a munkavállaló felett munkáltatói jogköröket ténylegesen gyakorló személy és – amennyiben a Társaságnál kinevezésre vagy megbízásra került, úgy – az adatvédelmi tisztviselő ellenőrizheti. Amennyiben ilyen személy megbízásra vagy kinevezésre kerül, úgy neve és elérhetősége az *1/1. sz. mellékletben* található.

A Társaság személyes adatot csak az érintett előzetes – különleges személyes adat esetén írásbeli – hozzájárulása vagy törvény, illetve törvényi felhatalmazás alapján kezel.

A Társaság az adat felvétele előtt minden esetben közli az érintettel az adatkezelés célját, valamint az adatkezelés jogalapját.

A Társaság szervezeti egységeinél adatkezelést végző alkalmazottak és a Társaság megbízásából az adatkezelésben résztvevő, annak valamely műveletét végző szervezetek alkalmazottjai kötelesek a megismert személyes adatokat üzleti titokként megőrizni.

Ha a szabályzat hatálya alatt álló személy tudomást szerez arról, hogy a Társaság által kezelt személyes adat hibás, hiányos vagy időszerűtlen, köteles azt helyesbíteni vagy helyesbítését az adat rögzítéséért felelős munkatársnál kezdeményezni.

A Társaság megbízásából adatfeldolgozói tevékenységet végző természetes vagy jogi személyekre, illetve jogi személyiséggel nem rendelkező szervezetekre vonatkozó adatvédelmi kötelezettségek az adatfeldolgozóval kötött megbízási szerződésben érvényesítendőek. Az adatfeldolgozóval a Társaság az Infotv. által előírt Adatfeldolgozói szerződést köt.

4. A TÁRSASÁG ADATVÉDELMI RENDSZERE

A Társaság vezető tisztségviselője a Társaság sajátosságainak figyelembevételével meghatározza az adatvédelem szervezését, az adatvédelemre, valamint az azzal összefüggő tevékenységre vonatkozó feladat- és hatásköröket, továbbá kijelöli az adatkezelés felügyeletét ellátó személyt.

A szabályzatban előírtak betartatásáért a feladatkörében minden érintett szervezeti egység vezetője felelős.

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

A Társaság adatvédelmi rendszerének felügyeletét a vezető tisztségviselő látja el egy általa kinevezett vagy megbízott adatvédelmi tisztviselő útján.

Az adatvédelmi tisztviselő szakmailag rátermett, az adatvédelmi jog és a gyakorlat szakértői szintű ismereteivel rendelkezik.

A Társaság az adatvédelmi tisztviselő nevét és elérhetőségét közzéteszi a honlapján, valamint bejelenti ezen adatokat a NAIH részére.

A Társaság biztosítja az adatvédelmi tisztviselő részére a feladat ellátásához szükséges forrásokat, valamint azt, hogy a feladatai ellátása során utasításokat senkitől ne fogadjon el, feladatai ellátásával összefüggésben szankcióval nem sújtható. Az adatvédelmi tisztviselő szervezetileg közvetlenül a Társaság vezető tisztségviselőjének tartozik felelősséggel.

Az adatvédelmi tisztviselő a vezető tisztségviselő közvetlen felügyeletével szervezi, irányítja és ellenőrzi a Társaság adatvédelmi és adatbiztonsági rendszerét.

A vezető tisztségviselő az adatvédelemmel kapcsolatosan:

a) felelős az érintettek Infotv-ben meghatározott jogainak gyakorlásához szükséges feltételek biztosításáért;
b) felelős a Társaság által kezelt személyes adatok védelméhez szükséges személyi, tárgyi és technikai feltételek biztosításáért;
c) felelős az adatkezelésre irányuló ellenőrzés során esetlegesen feltárt hiányosságok vagy jogszabálysértő körülmények megszüntetéséért, a személyi felelősség megállapításához szükséges eljárás kezdeményezéséért, illetve lefolytatásáért;
d) felügyeli az adatvédelmi tisztviselő tevékenységét;
e) vizsgálatot rendelhet el;
f) kiadja a Társaság adatvédelemmel kapcsolatos belső szabályait.

Adatvédelmi tisztviselő adatvédelemmel kapcsolatos feladatai:

a) segítséget nyújt az érintett jogainak biztosításában;
b) kezdeményezi a NAIH felé az Infotv-ben meghatározott nyilvántartásba vételi eljárás lefolytatását;
c) minden év január 30-ig jelentést készít a vezető tisztségviselő részére a Társaság adatvédelmi feladatainak végrehajtásáról;
d) jogosult jelen szabályzat betartását az egyes szervezeti egységeknél ellenőrizni;
e) vezeti az adatvédelmi incidens nyilvántartást;
f) részt vesz a NAIH által szervezett adatvédelmi tisztviselők konferenciáján;

g) figyelemmel kíséri az adatvédelemmel és információszabadsággal kapcsolatos jogszabályváltozásokat, ezek alapján indokolt esetben kezdeményezi jelen szabályzat módosítását;
h) közreműködik a NAIH-tól a Társasághoz érkezett megkeresések megválaszolásában és a NAIH által kezdeményezett vizsgálat, illetve adatvédelmi hatósági eljárás során;
i) általános állásfoglalás megadása céljából megkeresést fogalmaz meg a NAIH felé, amennyiben egy felmerült adatvédelmi kérdés jogértelmezés útján egyértelműen nem válaszolható meg;
j) tájékoztatást és szakmai tanácsot ad a Társaság adatvédelmi jogszabályokban előírt kötelezettségeinek ellátásával kapcsolatban;
k) ellenőrzi az adatvédelmi jogszabályoknak, valamint a Társaság belső szabályzatainak való megfelelést, ideértve a feladatkörök kijelölését, az adatkezelési műveletekben résztvevő személyek tudatosság-növelését és képzését, valamint a kapcsolódó auditokat is;
l) kérésre szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, valamint nyomon követi a hatásvizsgálat elvégzését;
m) együttműködik a NAIH-val;
n) az adatkezeléssel összefüggő ügyekben kapcsolattartó pontként szolgál a NAIH felé, valamint bármely egyéb kérdésben konzultációt folytat le.

Adatvédelmi incidens kezelése

Adatvédelmi incidens észlelése és jelentése

A Társaság minden munkavállalója – beleértve az egyéb jogviszonyban foglalkoztatott személyeket is – köteles a Társaságon belül történt adatvédelmi incidenst haladéktalanul jelenteni a szervezeti egysége vezetőjének, valamint az adatvédelmi tisztviselőnek. A bejelentés tartalmazza a bejelentő nevét, telefonszámát, beosztását, szervezeti egységének megnevezését, valamint az incidens tárgyát, rövid leírását és azt, hogy az incidens érinti-e a Társaság informatikai rendszerét.

Amennyiben az adatvédelmi incidens érinti a Társaság informatikai rendszerét is, akkor a bejelentést az IT vezetőnek is meg kell küldeni.

A bejelentés adatvédelmi tisztviselőhöz érkezését követően az adatvédelmi tisztviselő haladéktalanul megkezdi az adatvédelmi incidens kivizsgálását, értékelését és az incidenskezelési intézkedések foganatosítását.

Adatvédelmi incidens kivizsgálása, értékelése

Az adatvédelmi tisztviselő – informatikai rendszert érintő incidens esetén az IT vezetővel együttműködve
– megvizsgálja a bejelentést és amennyiben szükséges a bejelentőtől további adatokat kér az incidensre vonatkozóan. Az adatvédelmi tisztviselő felhívására a bejelentő köteles megadni: az adatvédelmi incidens bekövetkezésének időpontját és helyét, egyéb körülményeit, az általa érintett adatok körét, mennyiségét, az érintett személyek körét és számát, a várható hatásait, az adatvédelmi incidens megelőzésére, következményeinek enyhítésére megtett intézkedések felsorolását.

A bejelentő az adatszolgáltatást haladéktalanul, de legkésőbb 2 munkanapon belül teljesíti az adatvédelmi tisztviselő részére.

Amennyiben az ad atvédelmi incidens értékelése vizsgálatot igényel az adatvédelmi tisztviselő az IT vezetővel, valamint egyéb, a vizsgálat lefolytatásához szükséges munkatársak bevonásával lefolytatja a vizsgálatot.

A vizsgálatnak tartalmaznia kell, hogy az adatvédelmi incidens magas kockázattal jár-e az érintettek jogaira és szabadságaira, milyen jellegű kockázatról van szó, szükséges-e az érintettek tájékoztatása az incidensről. Amennyiben nem szükséges az érintettek tájékoztatása, a vizsgálatnak tartalmaznia kell ennek indokait is.

A vizsgálat eredményeként az adatvédelmi tisztviselő javaslatot tesz az adatvédelmi incidenssel érintett szervezeti egység vezetőjének az incidens kezeléshez szükséges intézkedések megtételére.

A javaslat alapján a megvalósítandó további intézkedésekről az adatok kezelését vagy feldolgozását végző szakterület vezetője – informatikai rendszerben bekövetkezett adatvédelmi incidens esetében az IT vezető egyetértésével - dönt.

A vizsgálatot legkésőbb a bejelentésnek az adatvédelmi tisztviselőhöz érkezésétől számított három munkanapon belül be kell fejezni és a vizsgálat eredményéről a Társaság vezető tisztségviselőjét az adatvédelmi tisztviselő tájékoztatja.

Az adatvédelmi incidens nyilvántartása

Az adatvédelmi incidensről az adatvédelmi tisztviselő nyilvántartást vezet.

A nyilvántartás tartalmazza:

- az érintett személyes adatok körét,
- az adatvédelmi incidenssel érintettek körét és számát,
- az adatvédelmi incidens időpontját,
- az adatvédelmi incidens körülményeit, hatásait,
- az elhárítására megtett intézkedéseket és
- egyéb jogszabályban előírt adatokat.

Az adatvédelmi incidens nyilvántartás pontos vezetéséről, aktualizálásáról az adatvédelmi tisztviselő gondoskodik.

Az adatvédelmi incidens bejelentése a Hatóság részére

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

A hatósági bejelentésnek tartalmaznia kell:

- az adatvédelmi incidenssel érintett adatok körét és hozzávetőleges számát,
- az adatvédelmi incidenssel érintett személyek körét és hozzávetőleges számát,
- az adatvédelmi incidens jellegét, körülményeit,
- az adatvédelemért felelős személy nevét és elérhetőségét,
- az adatvédelmi incidens valószínűsíthető következményeit és
- az adatvédelmi incidens orvoslására és enyhítésére megtett intézkedéseket.

Az érintettek tájékoztatása az adatvédelmi incidensről

Ha a vizsgálat eredményeként megállapítást nyert, hogy az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, ezért az érintettek tájékoztatása szükséges, az adatvédelmi tisztviselő haladéktalanul értesíti az érintetteket és a Társaság vezető tisztségviselőjét is.

Nem kell az érintetteket tájékoztatni:

- ha a Társaság olyan technikai, szervezési, védelmi intézkedéseket hajtott végre az érintett adatokra vonatkozóan, amelyek megakadályozzák az illetéktelen személyek számára való hozzáférést az adatokhoz vagy azok értelmezhetőségét;
- ha az adatvédelmi incidens bekövetkezését követően a Társaság olyan intézkedéseket tett, amelyek biztosítják, hogy a feltárt adatkezelési kockázat valószínűsíthetően nem valósul meg;
- ha a tájékoztatás aránytalan erőfeszítést tenne szükségessé. Ebben az esetben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, mely tájékoztatás elektronikus úton is megtörténhet.

Rendszeres tréningek

Az adatvédelmi tisztviselő gondoskodik az adatvédelmi tudatosság növelése érdekében adatvédelmi incidensekkel kapcsolatos oktatásról, mely során a múltban bekövetkezett adatvédelmi incidensek tapasztalatait, vagy a lehetséges adatvédelmi incidensek veszélyeit ismerteti, elemzi, a kockázatok csökkentésével, megelőzésével kapcsolatosan tájékoztatást ad, illetve az ismereteket ellenőrzi.

Hatásvizsgálat

Amennyiben valamely új adatkezelési folyamat – annak jellegére, hatókörére, körülményeire, céljaira tekintettel - valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, akkor az adatkezelés megkezdését megelőzően a Társaság hatásvizsgálatot folytat le arra vonatkozóan, hogy az adatkezelési folyamat a személyes adatok védelmét hogyan érinti. Egymáshoz hasonló adatkezelési műveletek, amelyek hasonló kockázatokat jelentenek egy hatásvizsgálat keretében is elvégezhetők.

A hatásvizsgálatot főszabály szerint az Adatkezelő végzi, a vizsgálat lefolytatásához kikéri az adatvédelmi tisztviselő szakmai tanácsát.

A hatásvizsgálat elvégzését követően szükség szerint, de legalább az adatkezelési műveletek által jelentett kockázat változása esetén az Adatkezelő gondoskodik a hatásvizsgálat felülvizsgálatáról, mely során a kockázatok értékelését újra elvégzi. A kockázatok felülvizsgálatát legalább 3 évente el kell végezni.

A személyes adatok kezelésével kapcsolatosan az Adatkezelő kötelezettsége továbbá a kockázatelemzés, amelynek lépései a következők:

- a személyes adatok kezelésével kapcsolatos kockázatok azonosítása,
- kockázati lista felállítása,
- az egyes kockázatok valószínűsíthető fő okainak és várható negatív hatásainak meghatározása, valamint
- ezek alapján a preventív és a korrektív kockázatkezelési folyamatok kidolgozása.

Szükséges a kockázatforrások feltárása, melyen belül meg kell határozni a kockázati preventív és korrektív célkezelés elemeit, az erőforrás-kezelés rendszerét, továbbá el kell különíteni az objektív és szubjektív kockázati elemeket.
Az elemzés során el kell jutni a teljes kockázatértékelési rendszer kialakításáig, amelyben teljes kockázatpotenciál és kockázat prioritási sorrend (nem az intézkedési rendszerrel azonos) megállapításának kell megtörténnie Az elemzés menetét és eredményeit írásba kell foglalni.

A kockázatpotenciálnál meg kell határozni a valószínűség szempontjából:
- kicsi
- közepes
- és nagy bekövetkezésű kockázatokat,

illetve horderő szempontjából:
- kicsi
- közepes
- és nagy horderejű kockázatokat.

Ez a meghatározás alapozza meg a későbbi kockázatkezelési eljárás módját mind a preventív, mind a korrektív eljárás tekintetében. A kockázatelemzés végrehajtásáért az adatvédelmi tisztviselő felel.

Előzetes konzultáció

Amennyiben az elvégzett hatásvizsgálat azt állapítja meg, hogy az adatkezelési folyamat valószínűsíthetően magas kockázattal jár, akkor a Társaság az adatkezelési folyamat megkezdését megelőzően szükség szerint konzultációt kezdeményez a Hatósággal.

A konzultáció kezdeményezése során a Társaság csatolja:
- az elvégzett hatástanulmányt,
- az adatvédelmi tisztviselő nevét, elérhetőségét,
- az adatkezelési folyamatban részt vevő adatkezelő(k), adatfeldolgozó(k) feladatköreinek felsorolását,
- az adatkezelés célját, módját és
- az érintettek jogainak, szabadságainak biztosítása védelmében hozott intézkedéseket, garanciákat.

Érdekmérlegelés

Az Infotv. rendelkezései szerint lehetőség van hozzájárulás nélküli adatkezelésre, ha ezt valamilyen jogos érdek lehetővé teszi, feltéve, hogy az Adatkezelő eleget tesz tájékoztatási kötelezettségének. Az adatkezelés jogalapjának vizsgálata során a GDPR 6. cikk (1) bekezdése a)-f) pontjai az irányadók.

Amennyiben a jogalapot a GDPR 6. cikk (1) bekezdés f) pontja jelenti, az adatkezelési folyamat, akkor és annyiban lesz jogszerű, amennyiben az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé.

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

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

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

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

A teszt eredményéről az érintettek tájékoztatást kapnak, melyből egyértelműen kiderül, hogy mely jogos érdek alapján és miért tekinthető arányos korlátozásnak az, hogy a Társaság az érintett beleegyezése nélkül kezeli a személyes adatot, tehát a Társaság adatkezeléséhez fűződő jogos érdeke miért múlja felül az érintett érdekeit, illetve jogait. A Társaság tájékoztatja az érintetteket a hozzájárulás hiányára tekintettel alkalmazott adatvédelmi garanciákról és az adatkezelés elleni tiltakozás lehetőségeiről.
Nem írható elő az ellentétes érdekek és jogok közötti súlyozás eredménye anélkül, hogy eltérő eredményt tenne lehetővé az Adatkezelő az adott eset sajátos körülményeire tekintettel, ezért minden egyes esetben külön érdekmérlegelési tesztet kell elvégezni.

Lehetséges forgatókönyv, melytől való eltérés jogát a Társaság fenntartja:
1. lépés: az Adatkezelő a tervezett adatkezelés megkezdése előtt áttekinti, hogy a célja elérése érdekében feltétlenül szükséges-e személyes adat kezelése: rendelkezésre állnak-e olyan alternatív megoldások, amelyek alkalmazásával személyes adatok kezelése nélkül megvalósítható a tervezett cél.
2. lépés: az Adatkezelő a jogos érdekét a lehető legpontosabban meghatározza.
3. lépés: az Adatkezelő meghatározza, hogy mi az adatkezelés célja, milyen személyes adatok, meddig tartó adatkezelését igényli a jogos érdek.
4. lépés: az Adatkezelő meghatározza, hogy az érintetteknek mik lehetnek az érdekeik az adott adatkezelés vonatkozásában (például azok a szempontok, amelyeket az érintettek felhozhatnának az adatkezeléssel szemben).
5. lépés: az Adatkezelő elvégzi jogos érdekeinek és az érintettek érdekeinek, alapjogainak súlyozását, ez alapján megállapítja, hogy a személyes adat kezelhető-e. A Társaság meghatározza, hogy miért korlátozza arányosan az Adatkezelő jogos érdeke – és az ennek alapján végzett adatkezelés – a 4. lépésben meghatározott érdekelti jogokat, várakozásokat.
6. lépés: az Adatkezelő meghatározza, mely garanciák biztosíthatják az adatkezelés szükségességét-arányosságát (természetesen más garanciális intézkedések is alkalmazhatók).

Személyazonosító igazolványok fénymásolása

A Társaság – összhangban a NAIH álláspontjával – nem készít fénymásolatot személyazonosító igazolványokról. A hatósági okmányról készített fénymásolat nem alkalmas a természetes személyek azonosítására, mivel az egyén személyes jelenléte elengedhetetlen a hatósági igazolvány alapján történő személyazonosításhoz. Az arcképes hatósági igazolvány értelemszerűen csak akkor rendelkezik bizonyító erővel, ha annak alapján a Társaság

megbizonyosodhat arról, hogy az igazolványon szereplő személy képmása és az igazolványt felmutató személy megegyeznek. Egy hatósági igazolványról készített másolat nem rendelkezik bizonyító erővel arról, hogy hiteles másolata egy érvényes hatósági igazolványnak.

5. ADATBIZTONSÁGI SZABÁLYOK

Fizikai védelem

A papíralapon kezelt személyes adatok biztonsága érdekében a Társaság az alábbi intézkedéseket alkalmazza:

- az adatokat csak az arra jogosultak ismerhetik meg, azokhoz más nem férhet hozzá, más számára fel nem tárhatóak;
- a dokumentumokat jól zárható, száraz, tűz- és vagyonvédelmi berendezéssel ellátott helyiségben helyezi el;
- a folyamatos aktív kezelésben lévő iratokhoz csak az illetékesek férhetnek hozzá;
- a Társaság adatkezelést végző munkatársa a nap folyamán csak úgy hagyhatja el az olyan helyiséget, ahol adatkezelés zajlik, hogy a rá bízott adathordozókat elzárja, vagy az irodát bezárja;
- a Társaság adatkezelést végző munkatársa a munkavégzés befejeztével a papíralapú adathordozót elzárja;
- amennyiben a papíralapon kezelt személyes adatok digitalizálásra kerülnek, a digitálisan tárolt dokumentumokra irányadó biztonsági szabályokat alkalmazza a Társaság.

Amennyiben a papíralapon tárolt személyes adat kezelésének célja megvalósult, úgy a Társaság intézkedik a papír megsemmisítéséről. Ebben az esetben a Társaság kijelöl egy munkavállalót, aki a megsemmisítésért felelős. A megsemmisítésért felelős munkavállaló a megsemmisítéssel érintett szervezeti egység bevonásával állítja össze a megsemmisítendő iratcsomagot. A megsemmisítésen háromtagú Megsemmisítési Bizottság vesz részt.

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

Informatikai védelem

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

- az adatkezelés során használt számítógépek a Társaság tulajdonát képezik, vagy azok fölött tulajdonosi jogkörrel megegyező joggal bír;
- a számítógépen található adatokhoz csak érvényes, személyre szóló, azonosítható jogosultsággal - legalább felhasználói névvel és jelszóval – lehet csak hozzáférni, a jelszavak cseréjéről a Társaság rendszeresen, illetve indokolt esetben gondoskodik;
- az adatokkal történő minden számítógépes rekord nyomon követhetően naplózásra kerül;
- a hálózati kiszolgáló gépen (a továbbiakban: szerver) tárolt adatokhoz csak megfelelő jogosultsággal és csakis az arra kijelölt személyek férhetnek hozzá;
- amennyiben az adatkezelés célja megvalósult, az adatkezelés határideje letelt, úgy az adatot tartalmazó fájl visszaállíthatatlanul törlésre kerül, az adat újra vissza nem nyerhető;

- A Társaság a hálózaton tárolt adatok biztonsága érdekében a szervereket magas rendelkezésre állású infrastruktúrával védi, az adatvesztést mentésekkel és archiválásokkal kerüli el;
- a személyes adatokat tartalmazó adatbázisok aktív adataiból napi mentést végez, amely a központi szerver teljes adatállományára vonatkozik és mágneses adathordozóra történik;
- a lementett adatokat tartalmazó mágneses adathordozó az erre a célra kialakított páncéldobozban tűzbiztos helyen és módon tárolja;
- a személyes adatokat kezelő hálózaton a vírusvédelemről folyamatosan gondoskodik;
- a rendelkezésre álló számítástechnikai eszközökkel, azok alkalmazásával megakadályozza illetéktelen személyek hálózati hozzáférését.

Jogosultságkezelés

A jogosultságkezelés szabályozásának célja, hogy a kiosztott jogosultságok pontosan nyomon követhetőek legyenek, dokumentált formában megőrzésre kerüljenek, valamint az egyes jogosultságokkal rendelkező személyek tevékenysége és az általuk felhasznált adatok köre ellenőrizhető legyen. Ezen adatok naprakészsége nagymértékben hozzásegíti a Társaságot a tőle elvárt, illetve általa elérhető biztonsági szint teljesítéséhez, továbbá az informatikai hálózat törvényi és szakmai normák szerinti üzemeltetéséhez. A szabályozás kiterjed az elektronikus megfigyelőrendszerek informatikai rendszerére és az azokhoz csatlakozó eszközökre is.
Az informatikai rendszerben a jogosultságok változásait (létező jogosultságok, azok módosítása, megszűnése, új jogosultságok kiosztása) dokumentálni kell.

A személyes adatok biztonsága érdekében a Társaság az alábbi jogosultságkezelési előírásokat alkalmazza:

- o Alapelvek
  - Új jogosultság beállítását, illetve jogosultság megváltoztatását a jogosultság birtokosának felhatalmazása alapján az IT felelős végzi.
  - A jogosultságok megállapítása során kizárólag a munkavégzéshez szükséges és elégséges jogosultságokat kell kiosztani.
  - El kell kerülni, hogy teljes hozzáférést, illetve adminisztrátori jogosultságokat kapjanak más munkát végző, illetve a jogosultság birtoklására igényt nem tartó személyek.
  - Adminisztrátori jogosultsággal rendelkező nevesített felhasználót kell alkalmazni a rendszer adminisztrálása érdekében minden esetben, ahol ez lehetséges.
  - Külső – karbantartó vagy fejlesztő – cég alkalmazottja folyamatosan működő, korlátlan időre szóló hozzáférési jogosultsággal nem rendelkezhet.

Jogosultságkezelési folyamat

Jogosultság igényléssel, módosítási igénnyel az IT felelőshöz lehet fordulni, a jogosultság kezelésekről az IT felelős nyilvántartást vezet.
Az IT felelős minden esetben konzultál a jogosultság birtokosával és az igénylő feletti munkáltatói jog gyakorlójával. A jogosultság megadásával vagy módosításával kapcsolatosan a vezető tisztségviselőnek és az igénylő feletti munkáltatói jog gyakorlójának vétójoga van.
A jogosultság birtokosának munka- vagy egyéb jogviszonya megszűnésével az IT felelős az addig birtokolt jogosultságait törli.
Az informatikai rendszerben a kilépő felhasználók profiljait fel kell függeszteni, használaton kívül kell helyezni. A felhasználói fiókok törlése a rendszerek ellenőrzését követően történhet meg, ha a törlés nem okoz adatvesztést.

6. ÁLNEVESÍTÉS

Az 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, mivel a Társaság az ilyen további információt külön tárolja, technikai és szervezési intézkedések megtételével biztosítja, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet kapcsolni.

Az álnéven történő adatkezelést a Társaság a nagyobb fokú biztonság érdekében, valamint a statisztikai célra gyűjtendő adatok, vagy a fejlesztés, tesztelés, karbantartás alatt álló rendszereknél a tesztadatok tekintetében végez, mivel a személyes adatok álnevesítése csökkentheti az érintettek számára a kockázatokat, valamint a Társaság ezáltal könnyebben meg tud felelni az adatvédelmi kötelezettségeinek.

Az álnevesítés személyes adatok kezelése során történő alkalmazásának ösztönzése céljából lehetővé teszi az álnevesítésre irányuló intézkedések és az általános elemzés egyidejű alkalmazását a Társaság szervezetén belül. A Társaság továbbá biztosítja, hogy az ahhoz szükséges további információkat, amelyek által a személyes adatokat egy adott érintetthez lehessen kapcsolni, elkülönítve tárolják. A Társaságnál az adatvédelmi tisztviselő az, aki ugyanazon a szervezeten belül feljogosított személynek minősül.

A természetes személyeket személyes adataik kezelése tekintetében megillető jogok és szabadságok védelme megköveteli a Rendelet követelményeinek teljesítését biztosító megfelelő technikai és szervezési intézkedések meghozatalát. Ahhoz, hogy az adatkezelő igazolni tudja a Rendeletnek való megfelelést, olyan belső szabályokat kell alkalmaznia, valamint olyan intézkedéseket kell végrehajtania, amelyek teljesítik, különösen a beépített és az alapértelmezett adatvédelem elveit.

A Társaság törekszik - a GDPR-nak való megfelelés érdekében - a személyes adatok kezelésének minimálisra csökkentésére, a személyes adatok mihamarabbi álnevesítésére, a személyes adatok funkcióinak és kezelésének átláthatóságára, valamint arra, hogy az érintett nyomon követhesse az adatkezelést, a Társaság pedig biztonsági elemeket hozhasson létre, illetve továbbfejleszthesse azokat.

7. BEÉPÍTETT ADATVÉDELEM

Bevezetésre kerül az ún. beépített adatvédelem (privacy by design), melynek következtében a Társaság már az adatkezelés tényleges megkezdése előtt is figyelemmel van a GDPR előírásaira. A beépített adatvédelem a Társaság saját, olyan belső eljárásainak az összessége, amivel - a külső szabályozásoktól függetlenül is - igyekszik megfelelni annak, hogy az érintett magánszféráját minél jobban védje.

A természetes személyeket személyes adataik kezelése tekintetében megillető jogok és szabadságok védelme megköveteli a GDPR követelményeinek teljesítését biztosító megfelelő technikai és szervezési intézkedések meghozatalát. Az említett intézkedések magukban foglalják a személyes adatok kezelésének minimálisra csökkentését, a személyes adatok mihamarabbi álnevesítését, a személyes adatok funkcióinak és kezelésének átláthatóságát, valamint azt, hogy az érintett nyomon követhesse az adatkezelést, a Társaság pedig biztonsági elemeket hozzon létre, illetve továbbfejleszthesse azokat. Az adatkezelésnek átláthatónak, felhasználó- központúnak, az adatvédelemnek proaktívnak kell lennie, az adat teljes életciklusát fel kell ölelnie, vagyis a teljes folyamatnak része kell hogy legyen.

A Társaság a tudomány és technológia állása, a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei, céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével, mind az adatkezelés módjának meghatározásakor, mind pedig az adatkezelés során olyan megfelelő technikai és szervezési intézkedéseket hajt végre, amelyek célja egyrészt az adatvédelmi elvek, például az adattakarékosság hatékony megvalósítása, másrészt a GDPR-ban foglalt követelmények teljesítéséhez és az érintettek jogainak védelméhez szükséges garanciák beépítése az adatkezelés folyamatába.

Technikai és szervezési intézkedések:

a) a személyes adatok álnevesítése és titkosítása;
b) a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének, integritásának, rendelkezésre állásának, ellenálló képességének biztosítása;
c) fizikai vagy műszaki incidens esetén az arra való képesség, hogy a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását kellő időben vissza lehet állítani;
d) az adatkezelés biztonságának garantálására hozott technikai és szervezési intézkedések hatékonyságának rendszeres tesztelése, felmérése és értékelése.

A Társaság megfelelő technikai és szervezési intézkedéseket hajt végre annak biztosítására, hogy alapértelmezés szerint kizárólag olyan személyes adatok kezelésére kerüljön sor, amelyek az adott konkrét adatkezelési cél szempontjából szükségesek. Ez a kötelezettség vonatkozik a gyűjtött személyes adatok mennyiségére, kezelésük mértékére, tárolásuk időtartamára és hozzáférhetőségükre. Ezeknek az intézkedéseknek különösen azt kell biztosítaniuk, hogy a személyes adatok alapértelmezés szerint természetes személy beavatkozása nélkül ne válhassanak hozzáférhetővé meghatározatlan számú személy számára.

A GDPR 42. cikke szerinti jóváhagyott tanúsítási mechanizmus felhasználható annak bizonyítása részeként, hogy a Társaság teljesíti az előbbiekben előírt követelményeket.

A Társaság intézkedéseket hoz annak biztosítására, hogy a személyes adatokhoz hozzáféréssel rendelkező természetes személyek kizárólag az utasításoknak megfelelően kezelhessék a személyes adatokat, kivéve, ha az ettől való eltérésre uniós vagy tagállami jog kötelezi őket.

A beépített és az alapértelmezett adatvédelem elveit a közbeszerzések során is figyelembe veszi a Társaság.

Adattovábbítás esetén a megfelelőségi határozat hiányában a Társaság vagy az adatfeldolgozó a megfelelő garanciák érintett számára való biztosítása útján gondoskodik az adatvédelem harmadik országbeli hiányosságainak ellensúlyozásáról. A garanciák biztosítják az adatvédelmi követelményeknek való megfelelést, hogy az Európai Unión belüli adatkezelés esetén biztosított jogokkal azonos szintű jogokat biztosítanak az érintettek számára, beleértve az érintettek jogainak érvényesíthetőségét és a hatékony jogorvoslat lehetőségét, ezen belül ideértve azt, hogy az érintettek hatékony közigazgatási vagy bírósági jogorvoslatot vehessenek igénybe, továbbá kártérítést igényelhessenek az Európai Unióban vagy egy harmadik országban. A garanciák különösen a személyes adatok kezelésére vonatkozó általános elveknek, valamint a beépített és alapértelmezett adatvédelem elveinek való megfelelésre vonatkoznak.

8. OKTATÁS ÉS TRÉNINGRENDSZER

Kiemelt területként kell kezelni a munkavállalók kapcsán a biztonságtudatossági képzést a szervezet informatikai és nem informatikai alkalmazottai részére.

A biztonságtudatos magatartás komoly üzleti károkat okozó hibák és támadások megelőzésében játszhat szerepet.

Nem elegendő a megfelelően kidolgozott IT biztonsági szabályzat, információbiztonsági rendelkezések és adatvédelmi, adatbiztonsági szabályozás megléte a szervezetben, a munkavállalókban rendszeres képzések, tréningek során kell tudatosítani, hogy a kialakított szabályrendszer és az IT eszközök önmagukban nem képesek garantálni a szervezet számára az adat- és információbiztonságot, ehhez a napi munkatevékenységük során felelős magatartásukkal a dolgozóknak is hozzá kell járulniuk.

A munkavállalók megfelelő képzése a képzést követően kimutathatóan kevesebb biztonsági incidenst eredményez, ami a közvetlen adatvesztésből és esetleges adatvédelmi birságból eredő károkon túl a pénzügyi eredményekben is nyilvánvalóan megmutatkozik.

Amunkavállalók általános adatvédelmi-információbiztonsági tréning rendje hathavonta (kapcsolható más rendszeres képzésekhez, tréningekhez pl. tűz- és munkavédelem) egy óra időtartamban történjen. Ez vonatkozik az informatikai és nem informatikai munkavállalókra egyaránt.

Külön tréningrendet kell biztosítani az informatikai, különösen a rendszergazdai feladatokat ellátók részére. Ennek célja, hogy kizökkentse a képzés alatt állókat a megszokott munkamenetükből és feltárja előttük a rosszindulatú támadások, hekkerek által folyamatosan fejlesztett aktuális támadási szemléletet, rámutasson az aktuális trendek szerint jellemzően keresett gyenge pontokra, segítse őket abban, hogy érzékelt behatolási kísérlet esetén milyen megoldásokat preferáljanak a támadások elhárítására és a kockázat alacsony szinten tartásának érdekében.

10. AZ ÉRINTETTEK JOGAINAK ÉRVÉNYESÍTÉSE

Az érintett tájékoztatást kérhet személyes adatai kezeléséről, valamint kérheti személyes adatainak helyesbítését, illetve – a jogszabályban elrendelt adatkezelések kivételével – törlését a Társaság feltüntetett elérhetőségein.

Az érintett jogosult arra, hogy a rá vonatkozó, általa az Adatkezelő rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel írott olvasható formában megkapja, továbbá jogosult arra, hogy ezeket az adatokat egy másik adatkezelőnek továbbítsa.

A Társaság a beérkezett kérelmet, illetve tiltakozást köteles a beérkezéstől számított három napon belül áttenni az adatkezelés szempontjából feladat- és hatáskörrel rendelkező szervezeti egység vezetőjéhez.

A feladat- és hatáskörrel rendelkező szervezeti egység vezetője az érintett személyes adatának kezelésével összefüggő kérelmére, az érkezésétől számított legkésőbb 25 – tiltakozási jog gyakorlása esetén 15 – napon belül írásban, közérthető formában választ ad.

A tájékoztatás kiterjed az Infotv. 15. § (1) bekezdésében meghatározott információkra, amennyiben az érintett tájékoztatása törvény alapján nem tagadható meg.

A tájékoztatás főszabály szerint ingyenes, költségtérítést Társaság csak az Infotv. 15. § (5) bekezdésében meghatározott esetben számít fel.

A Társaság kérelmet csak az Infotv. 9. § (1) bekezdésében vagy a 19. §-ában meghatározott okokból utasít el, erre csak indoklással, az Infotv. 16. § (2) bekezdésében meghatározott tájékoztatással, írásban kerül sor.

A valóságnak nem megfelelő adatot az adatot kezelő szervezeti egység vezetője – amennyiben a szükséges adatok és az azokat bizonyító közokiratok rendelkezésre állnak – helyesbíti, az Infotv. 17. § (2) bekezdésében meghatározott okok fennállása esetén intézkedik a kezelt személyes adat törlése iránt.

Az érintett személyes adata kezelése elleni tiltakozásának elbírálási időtartamára – de legfeljebb 5 napra – az adatkezelést az adatkezelést végző szervezeti egység vezetője felfüggeszti, a tiltakozás megalapozottságát megvizsgálja és döntést hoz, amelyről a kérelmezőt az Infotv. 21. § (2) bekezdésében foglaltak szerint tájékoztatja.

Amennyiben a tiltakozás indokolt, az adatot kezelő szervezeti egység vezetője az Infotv. 21. § (3) bekezdésében meghatározottak szerint jár el.

Amennyiben az érintett jogainak gyakorlása során az ügy megítélése nem egyértelmű, az adatot kezelő szervezeti egység vezetője az ügy iratainak és az ügyre vonatkozó álláspontjának megküldésével állásfoglalást kér az adatvédelmi tisztviselőtől, aki azt három napon belül teljesíti.

A Társaság az érintett adatainak jogellenes kezelésével vagy az adatbiztonság követelményeinek megszegésével másnak okozott kárt, illetve az általa vagy az általa igénybe vett adatfeldolgozó által okozott személyiségi jogsértés esetén járó sérelemdíjat is megtéríti. Az Adatkezelő mentesül az okozott kárért való felelősség és a sérelemdíj megfizetésének kötelezettsége alól, ha bizonyítja, hogy a kárt vagy az érintett személyiségi jogának sérelmét az adatkezelés körén kívül eső, elháríthatatlan ok idézte elő.

Ugyanígy nem téríti meg a kárt, amennyiben az a károsult szándékos vagy súlyosan gondatlan magatartásából származott.

Az érintett a jogorvoslati lehetőséggel, panasszal az Adatkezelőnél, az adatkezelő adatvédelmi tisztviselőjénél, a lakóhelye vagy tartózkodási helye szerinti illetékes törvényszéknél vagy a Nemzeti Adatvédelmi és Információszabadság Hatóságnál (1125 Budapest, Szilágyi Erzsébet fasor 22/C.) élhet.

11. A TÁRSASÁGNÁL MEGVALÓSULÓ ADATKEZELÉSEK

Az adatkezelés helye:
8640 Fonyód, Vágóhíd u. 17.

11.1. SZOLGÁLTATÁSI TEVÉKENYSÉGGEL ÖSSZEFÜGGŐ ADATKEZELÉS

A Társaság fő tevékenysége a közfoglalkoztatás, városüzemeltetés, a helyi közutak és strandok karbantartása.

Közfoglalkoztatás

- A Fonyódi Városfejlesztési és Városüzemeltetési Nonprofit Közhasznú Kft., mint munkáltató foglalkoztat közfoglalkoztatottakat a közfoglalkoztatásról szóló 2011. évi CVI. törvény alapján. Ezen foglalkoztatottak adatait a Társaság adatkezelőként kezeli.

A közfoglalkoztatottak adatkezelései jelen szabályzat 11.6 fejezetében kerülnek részletesen szabályozásra, ezért az abban foglalt szabályok az irányadók.

Városüzemeltetési feladatok,

A városüzemeltetési feladatok körébe tartozik:

- Zöldterület-gondozás, parkfenntartás
- Zöldhulladék elszállítása
- Zászlózási feladatok
- Útkarbantartás
- Karácsonyi díszkivilágítás üzemeltetése
- A város strandjainak karbantartása, ellenőrzése
- Autóbusz várók karbantartása
- Mezőgazdasági tevékenység
- szállítmányozás, gépbérlés

Ügyfelek személyes adatainak, szerződéses adatoknak a felvétele (magánszemélyek, egyéni vállalkozók) papír alapon történik.

Az ügyfeleknek történő számlázást saját alkalmazott végzi, azonban a könyvelés megbízott külső cég rendszerében történik, mely cég így adatfeldolgozó.
Az adatok feldolgozása Adatfeldolgozói Szerződés alapján történik.

adatkezelés célja: A szolgáltatások teljesítéséhez szükséges személyes adatok kezelése.

kezelt adatok köre: magánszemély, illetve egyéni vállalkozó neve, számlázási címe, elérhetőségi adatai.

adatkezelés jogalapja: az érintet hozzájárulása (Info törvény 5 § (1) bekezdés a)pontja).

adattárolás módja: elektronikusan a Társaság informatikai rendszerében és papír alapon.

11.2. BEJELENTÉSSEL ÖSSZEFÜGGŐ ADATKEZELÉS

A Városüzemeltetési tevékenység kapcsán kifejezett ügyfélszolgálat nem működik, de bejelentési lehetőség van, melynek helye:
8640 Fonyód, Vágóhíd u. 17.

Telefonon is lehet bejelentést tenni a Társaság megadott elérhetőségi telefonszámán.

Elektronikus levélben a megadott központi e-mail címen a Társaság elektronikus formában is fogad bejelentéseket.

Az ügyelek által igénybe vehető bejelentés módjai:

a) személyesen
b) telefonon: telefonos ügyintézés (ügyfél neve, címe és telefonszáma rögzítésre kerül)
c) Elektronikus levélben (ügyfél neve, címe és elérhetősége rögzítésre kerül).

Amennyiben a bejelentésről jegyzőkönyv készül, az a következőket tartalmazza:

a) az ügyfél neve;
b) az ügyfél lakcíme, székhelye, illetve amennyiben szükséges, levelezési címe;
c) a bejelentés előterjesztésének helye, ideje, módja;
d) az ügyfél bejelentésének részletes leírása, a bejelentéssel érintett kifogások elkülönítetten történő rögzítésével, annak érdekében, hogy az ügyfél bejelentésében foglalt valamennyi kifogás teljes körűen kivizsgálásra kerüljön;
e) az ügyfél által bemutatott iratok, dokumentumok és egyéb bizonyítékok jegyzéke;
f) a jegyzőkönyvet felvevő személy és az ügyfél aláírása
g) a jegyzőkönyv felvételének helye, ideje.

adatkezelés célja: ügyfélpanaszok felvétele, szolgáltatási tevékenységgel összefüggő panaszkezelés intézése az Adatkezelőnél,

kezelt adatok köre: neve, ügyfélszám, lakcíme, székhelye, levelezési címe, telefonszáma;, értesítés módja, panasszal érintett szolgáltatás panasz leírása, oka, panaszos igénye, a panasz alátámasztásához szükséges, az ügyfél birtokában lévő olyan dokumentumok másolata, amely a szolgáltatónál nem áll rendelkezésre, meghatalmazott útján eljáró ügyfél esetében érvényes meghatalmazás, a panasz kivizsgálásához, megválaszolásához szükséges egyéb adat;

adatkezelés jogalapja: érintett hozzájárulása (az Infotv. 5. § (1) a); a fogyasztóvédelemről szóló 1997. évi CLV. törvény 17/B (3) bekezdése

adattárolás határideje: a panasz megválaszolásától számított fogyasztóvédelmi törvény szerinti 5 év;

adattárolás módja: elektronikus és papíralapú.

11.4. INFORMATIKAI, ELEKTRONIKUS ADATKEZELÉS

A Társaság saját honlappal rendelkezik, amely a http://www.fonyodert.hu címen érhető el.

A honlapon automatikus adatgyűjtés nem valósul meg.

A látogatók a honlapon található telefonszámon, illetve e-mail címen keresztül léphetnek kapcsolatba a Társasággal.

A társaság honlapját megbízott külső cég üzemelteti. Tárhely szolgáltató szintén megbízott cég.

adatkezelés célja: panaszkezelés céljából az aktuális hírekről szóló értesítések érdekében történő azonosítás;

kezelt adatok köre: e-mail cím, IP cím;

adatkezelés jogalapja: Infotv.5. § (1) a) pontja szerinti érintetti hozzájárulás;

adattárolás határideje: az adatkezelési cél megvalósulásáig;

adattárolás módja: elektronikus.

11.6. SZEMÉLYÜGYI ADATKEZELÉS

11.6.1. MUNKAVÁLLALÓK MUNKAVISZONNYAL ÖSSZEFÜGGŐ ADATKEZELÉSE

A munkavállalók személyes adatainak kezelésére vonatkozóan az alábbiak szerint jár el a társaság:

Az adatok a Mt. szerinti adatkörben különös tekintettel a 2012. évi I. tv. 10-11. §-ában meghatározottak szerint kezelhetők.

Ezenkívül a közfoglalkoztatott személyek foglalkoztatása esetében a foglalkoztatás jogalapja még a közfoglalkoztatásról és a közfoglalkoztatáshoz kapcsolódó, valamint egyéb törvények módosításáról szóló 2011. Évi CVI. törvény 2-4 §-a.

adatkezelés célja: munkaviszony létesítése, teljesítése vagy megszüntetése, az ezekkel kapcsolatos jogosultságok elismerése és kötelezettségek tanúsítása

kezelt adatok köre:

munkavállaló kapcsán: neve, születési neve, születési helye és ideje, állampolgársága, törzsszáma, anyja születési neve, lakóhelyének címe, tartózkodási helye (amennyiben eltérő a lakóhelytől), magán-nyugdíjpénztári tagság ténye, belépés ideje (év, hó, nap), magánnyugdíjpénztár neve és kódja, adóazonosító jele, társadalombiztosítási azonosító jele (TAJ szám), nyugdíjas törzsszám (nyugdíjas munkavállaló esetén), folyószámla száma, munkaviszony kezdő napja, biztosítási jogviszony típusa, heti munkaórák száma, telefonszáma, családi állapota, végzettséget igazoló okmány másolati példánya, munkaalkalmassági egészségügyi igazolás, munkaköre, orvosi alkalmasság ténye, erkölcsi bizonyítványa, kiállításának dátuma, okmányszáma, kérelem azonosítója, a leszámolást

követően a munkaköri alkalmassági záró orvosi vizsgálat elvégzésének ténye, meghatározott munkakörben vezetési engedély kategóriánkénti egészségügyi alkalmassága lejártának időpontja, főálláson kívüli munkavégzés esetén a jogviszony jellege, a munkáltató neve és székhelye, a főálláson kívüli munkahelyen teljesített havi átlagos munkaidő, elvégzendő tevékenység.

adatkezelés jogalapja: törvényi felhatalmazás [a munka törvénykönyvéről szóló 2012. évi I. törvény 10. § (1) és (3)] és az érintett hozzájárulása [Infotv. 5 § (1) a) és 6. § (6)]; A társadalombiztosítás ellátásairól és magánnyugdíjra jogosultakról, valamint e szolgáltatások fedezetéről szóló 1997. évi LXXX. Törvény; A kötelező egészségbiztosítási ellátásról szóló 1997. évi LXXXIII. törvény; A személyi jövedelemadóról szóló 1995. évi. CXVII. Törvény; a közfoglalkoztatásról szóló 2011. évi CVI. törvény 2-4. §.

adattárolás határideje: az adatkezelés céljának megvalósulásáig, főszabály szerint munkaviszonnyal kapcsolatos jogosultságokkal és kötelezettségekkel kapcsolatosan a munkaviszony megszűnéséig, munkaviszonyból fakadó jogosultságokkal kapcsolatosan a nyugdíjfolyósításról szóló jogszabályokban meghatározott határideig

adatkezelés módja: elektronikus és papír alapon

11.6.2. MUNKAVÁLLALÓK ELLENŐRZÉSÉVEL ÖSSZEFÜGGŐ ADATKEZELÉS

A munkáltató ellenőrizheti a munkavállalókat a munkaviszonyból eredő kötelezettségek teljesítése céljából munkaviszonnyal összefüggő magatartása körében. Az ellenőrzésre a munka törvénykönyve [11.§ (1)-(2)] ad jogalapot.

A Társaságnál bizonyos beosztásokhoz céges telefont és e-mail címet kapnak a munkavállalók. Az irodai dolgozók számára a cég számítógépet is biztosít.

A céges mobiltelefonok első sorban munkavégzés céljára kerülnek használatba adásra.

Mivel a Társaság tulajdonát képező személyi számítógépeket és laptopokat, céges e-mail címeket a cég munkavégzés céljából biztosítja, így amennyiben a munkavállaló ezen eszközökön magáncélú személyes adatait (pl.: családi fotók, telefonkönyvek, saját adatbázisok stb.) tárolja, úgy a Társaság a számítógép ellenőrzése során ezeket az adatokat is megismerheti. Ezen adatkezelés ellen kifogással nem élhet a munkavállaló, mert a nem munkavégzés céljából történő, de a társasági eszközön való személyes adatok tárolása az adatkezeléshez történő Infotv. 5. § (1) a) szerinti érintetti hozzájárulásnak minősülnek. Erről (illetve az archiválás és a rendszergazdai tevékenység tényéről) a munkavállalókat az eszközök használatba adása előtt írásban tájékoztatja a Társaság.

Mindazon e-mail címek, amelyekben a Társaság neve kiterjesztésként benne foglaltatik (... @fonyodert.hu), a Társaság tulajdonát képezik. Ezen címeken a Társaság munkavállalói által folytatott levelezés munkacélú levelezésnek minősül. Az ilyen címeken folytatott levelezésbe a Társaság megfelelő jogalap esetén jogosult betekinteni. A Társaság jogosult a fent nevezett címeken folytatott levelezések meghatározott időközönkénti biztonsági mentésére, az elektronikus levelező rendszer folyamatosságának és stabilitásának érdekében adatbiztonsági okokból saját eszközein bármilyen állomány törlésére.
Amennyiben a munkavállaló „...@fonyodert.hu" céges e-mail címén található leveleiben magáncélú személyes adatait tárolja, úgy a Társaság az e-mail cím ellenőrzése során ezeket az adatokat is megismerheti. Ezen adatkezelés ellen kifogással nem élhet a munkavállaló, mert a

nem munkavégzés céljából történő, de a társasági e-mail címen való személyes adatok tárolása az adatkezeléshez történő Infotv. 5. § (1) a) szerinti érintetti hozzájárulásnak minősülnek.
A munkáltató jogosult ellenőrizni a munkahelyi postafiókot és internet használatot. Mindemellett főszabály szerint a magáncélú levelek tartalmát a munkáltató munkaviszonyból fakadó jogosultság érvényesítése során sem jogosult megismerni.

adatkezelés célja: a Társaság jogos üzleti érdekeinek megfelelően a munkavállalók Mt. 11. § (1)(2) bekezdése szerinti ellenőrzése, így különösen a munkavállalónak biztosított számítógép, e-mail cím, telefonhasználat és internet-hozzáférés ellenőrzése.

kezelt adatok köre: az ellenőrzés során rögzített személyes adatok, így különösen magán e-mail címek, magán telefonszámok, fényképek, saját számítógépes dokumentumok, internetes böngészési előzmények, cookie-k, munkajogviszony ellátása során észlelt jogsértés ténye, a jogsértés leírása.

adatkezelés jogalapja: Mt. 11. § (1) (2) bekezdése és esetlegesen Infotv. 5. § (1) a)

adattárolás határideje: az adatkezelés céljának megvalósulásáig.

11.6.3. MUNKÁRA JELENTKEZŐK ADATKEZELÉSE

A Társasághoz toborzás útján érkeznek be önéletrajzok az alábbi metodika szerint:

a közfoglalkoztatottak a munkaügyi csoportnál jelzik munkába állási szándékukat. A Társaság telefonon értesíti őket a lehetőségről és a Munkaügyi Központ közvetíti ki őket.

Egyéb, saját munkavállaló jelentkezésére vonatkozó szabályok

Amennyiben a Társaság állás betöltésére ír ki pályázatot, azt minden esetben a Fonyódi Városfejlesztési és Városüzemeltetési Nonprofit Közhasznú Kft. intézi, hirdetések útján (újság, internet) toborozza a lehetséges jelölteket.
A jelentkezők a Fonyódi Városfejlesztési és Városüzemeltetési Nonprofit Közhasznú Kft-hez küldik be önéletrajzaikat. Az alkalmas jelölt munkába állását követően a munkavállaláshoz szükséges adatai átkerülnek a Fonyódi Városfejlesztési és Városüzemeltetési Nonprofit Közhasznú Kft-hez. Az önéletrajzok a Fonyódi Városfejlesztési és Városüzemeltetési Nonprofit Közhasznú Kft-nél eltárolásra kerülnek.

A munkaerő-toborzásra vonatkozó különös szabályok

A Társaság az önéletrajzokat főszabály szerint a későbbi felhasználás céljából tárolja – igaz ez abban az esetben is, ha az önéletrajz konkrét meghirdetett pozíció betöltése céljából érkezett. Az önéletrajzokat és az azon szereplő személyes adatokat a Társaság jelen szabályzat alapján és az abban foglaltak szerint kezeli. Amennyiben az érintett nem kívánja, hogy a későbbiekben az itt meghatározottak szerinti határidőn belül kezelje a Társaság az adatait, úgy ezt vagy az önéletrajz megküldésével egyidejűleg jeleznie kell vagy a későbbiek során visszavonni az önéletrajz beküldésével megadott hozzájárulását. (Mivel jelen szabályok az érintettek számára az önéletrajz megküldése előtt is elérhetőek, így az erre vonatkozó előzetes tájékoztatást megadottnak tekinthető, a hozzájárulást pedig önkéntes.)

adatkezelés célja: a megüresedő álláshelyek betöltésére megfelelő leendő munkavállaló kiválasztása, a jelentkezők személyes adatainak kezelése

kezelt adatok köre: név, születési dátum, anyja neve, lakcím, képzési adatok, fénykép, az érintett által megadott egyéb adatok

adatkezelés jogalapja: az Infotv. 5 § (1) a) szerinti érintetti hozzájárulás

adattárolás határideje: az adatfelvételtől számított 1 évig

adattárolás módja: elektronikusan és papír alapon

12. AZ ÉRINTETTEK JOGAI ÉS JOGÉRVÉNYESÍTÉSI LEHETŐSÉGEIK

12.1. Az érintett jogosult tájékoztatást kérni az Adatkezelő által kezelt, rá vonatkozó személyes adatokról, továbbá kérheti azok módosítását, illetve törlését, törvényben meghatározott módon.

12.2. Adatkezelő az érintett kérésére tájékoztatást ad a rá vonatkozó, általa kezelt adatokról, az adatkezelés céljáról, jogalapjáról, időtartamáról, továbbá az esetleges adattovábbítás céljáról, indokáról, jogalapjáról.

Adatkezelő a kérelem benyújtásától számított 30 napon belül írásban adja meg a kért tájékoztatást.

12.3. Érintett bármely, az adatkezeléssel kapcsolatos kérdéssel, illetve észrevétellel az Adatkezelőhöz, illetve adatkezelő munkatársához – adatvédelmi tisztviselőhöz - fordulhat a szabályzat végén található elérhetőségeken keresztül.

12.4. Az érintett bármikor jogosult a helytelenül rögzített adatainak helyesbítését vagy azok törlését kérni. A törlés nem vonatkozik a jogszabály alapján szükséges adatkezelésekre, azokat adatkezelő a szükséges időtartamig megőrzi.

12.5. Az érintett az adatvédelemre vonatkozó törvények alapján bíróság előtt érvényesítheti jogait. Lehetősége van továbbá a Nemzeti Adatvédelmi és Információszabadság Hatósághoz (NAIH) (1125 Budapest, Szilágyi Erzsébet fasor 22/C) fordulni.

12.6. Amennyiben az érintett az adatrögzítés során szándékosan téves, félrevezető adatokat adott meg vagy bármilyen más módon kárt okozott, az adatkezelő jogosult az érintettel szemben jogi lépést, kártérítési igényt érvényesíteni. Az adatkezelő ilyen esetben minden tőle telhető segítséget megad az eljáró hatóságoknak a jogsértő személy személyazonosságának megállapítása céljából.

13. AZ ADATKEZELÉSI SZABÁLYZAT MÓDOSÍTÁSA

Az adatkezelő fenntartja magának a jogot, hogy a jelen Adatvédelmi Szabályzatot egyoldalú döntésével bármikor módosítsa. A jelen szabályzat módosítását követően valamennyi érintettet az adatkezelő megfelelő módon tájékoztat. Az érintettek a megváltozott adatkezelési szabályokat tudomásul veszik, ezen túlmenő beleegyezésük kikérésére nincs szükség.

13.1. KAPCSOLÓDÓ SZABÁLYZATOK

Jelen szabályzattal együtt kezelendők az alábbi szabályzatok:

- Iratkezelési Szabályzat

14. AZ ADATKEZELŐ ÉS AZ ADATVÉDELMI TISZTVISELŐ ELÉRHETŐSÉGEI

Adatkezelő:

Fonyódi Városfejlesztési és Városüzemeltetési Nonprofit Közhasznú Kft.

8640 Fonyód, Vágóhíd u. 17.

Tel.: +36 85 560 287

Adatvédelmi tisztviselő:

Tóth Szabolcs
e-mail: toth.szabolcs@fonyod.hu
+36 85 562 980

Az adatszolgáltatási nyilvántartási mintát e szabályzat 1. melléklete tartalmazza.

Jelen szabályzat hatálybalépése: 2018. május 24.

Fonyód, 2018. május 24.

Fonyódi Városfejlesztési és Városüzemeltetési Nonprofit Közhasznú Kft. 8640 Fonyód, Vágóhíd u. 17. Adószám: 23793121-2-14 · Cégj.sz: 14-09-312254 OTP Bank Nyrt.: 11743093-20019529

Kristóf Györgyné

ügyvezető igazgató

1. sz. melléklet

Adatkezelő nyilvántartási azonosítója	Adatszolgáltatás ideje	Adatszolgáltatás célja, jogalapja	Adatszolgáltatást kérő neve	Szolgáltatott adatok köre