



FŐKÉTÜSZ FŐVÁROSI
KÉMÉNYSEPRÓIPARI KFT.
 **BUDAPEST**

A FŐKÉTÜSZ Kft. Adatvédelmi és Adatbiztonsági Szabályzata (Kivonat – Mellékletek nélkül honlapon történő közzététel céljából)

Kelt: Budapest, 2018.07.19.

Tartalomjegyzék

1. A szabályzat célja és hatálya	1
2. Fogalmak	2
3. Az adatkezelések szabályai	5
4. A Társaság adatvédelmi rendszere	5
5. Adatvédelmi incidens kezelése	7
___ 5.1. Adatvédelmi incidens észlelése és jelentése	7
___ 5.2. Adatvédelmi incidens kivizsgálása, értékelése	8
___ 5.3. Az adatvédelmi incidens nyilvántartása	8
___ 5.4. Az adatvédelmi incidens bejelentése a Hatóság részére	8
___ 5.5. Az érintettek tájékoztatása az adatvédelmi incidensről	9
6. Rendszeres tréningek	9
7. Hatásvizsgálat	9
8. Előzetes konzultáció	10
9. Érdekmérlegelés	10
10. Adatbiztonsági szabályok	11
___ 10.1. Fizikai védelem	12
___ 10.2. Informatikai védelem	12
___ 10.3. Szerverek biztonsága	13
11. Jogosultságkezelés	13
___ 11.1. Jogosultságkezelési folyamat	14
12. Álnevesítés	14
13. Beépített adatvédelem	-17 -
14. Mobil eszköz menedzsment	16
15. Oktatás és tréningrendszer	17
16. Az érintettek jogainak érvényesítése	17
17. A Társaságnál megvalósuló adatkezelések	19
18. Közszolgáltatási tevékenységgel összefüggő adatkezelések	19
19. Ügyfélszolgálati tevékenységgel összefüggő adatkezelés	20
20. Hátralékkezelés	21
21. Piaci szolgáltatása kapcsolatos adatkezelések	21
___ 21.1. Nem lakossági szektornak történő szolgáltatás	21
22. Webshop üzemeltetés	22
23. Személyügyi adatkezelések	22
___ 23.1. A Társasághoz történő jelentkezés folyamata	22
___ 23.2. Fejvadász cégen keresztül érkező jelentkezés	- 24 -
___ 23.3. Hirdetésen keresztül történő jelentkezés	- 24 -
___ 23.4. A nem meghirdetett álláshelyre való jelentkezéssel és a munkaerő-toborzással kapcsolatos közös szabályok	22
___ 23.5. A nem meghirdetett álláshelyre való jelentkezésre vonatkozó különös szabályok	22
___ 23.6. Az ajánlás útján érkező önéletrajzokra vonatkozó különös szabályok	23
24. Munkaviszonnyal kapcsolatos adatkezelés	23
___ 24.1. Munkakör betöltéséhez szükséges orvosi vizsgálat	25
___ 24.2. A munkaviszony fenntartásával és megszűnésével kapcsolatos adatkezelések	25
___ 24.3. A munkaviszonnyal kapcsolatos adatkezelésekre vonatkozó nyilatkozatok	26
___ 24.4. Munkavállalók oktatása	26
___ 24.5. Béren kívüli juttatások	28

___ 24.6. Szociális támogatási rendszerek	28
24.7. Harmadik személyek munkaviszonnyal kapcsolatosan megadott adatai-	28 -
24.8. Munkavégzésre irányuló egyéb munkaviszonyban foglalkoztatott személyek adatkezelése	- 30 -
24.9. Diák munkavállalók adatkezelése	- 30 -
25. A munkavállalók ellenőrzésével kapcsolatos adatkezelés	28
___ 25.1. Céges eszközök ellenőrzése	29
___ 25.2. Céges e-mail címek ellenőrzése	29
___ 25.3. Céges telefonhasználat	29
___ 25.4. Az ellenőrzés menete	29
___ 25.5. GPS alkalmazása	30
26. Céges biztosítással kapcsolatos adatkezelés	30
27. Elektronikus megfigyelőrendszer alkalmazása	- 32 -
___ 27.1. Kamerafigyeléssel összefüggő adatkezelés	31
27.2. Az elektronikus megfigyelőrendszerrel készített felvételek törlésének módja és határideje	- 34 -
___ 27.3. Az elektronikus megfigyeléssel kapcsolatos garanciális szabályok	32
27.4. Az érintettek tájékoztatása	- 34 -
___ 27.5. A Társaság munkavállalóinak tájékoztatása	32
___ 27.4. A kameraképek megtekintése	33
___ 27.5. A kameraképek zárolása	33
___ 27.6. Zárolási jogosultsággal rendelkező személyek	33
27.6. I. szektor	- 35 -
27.7. II. szektor	- 36 -
27.8. III. szektor	- 36 -
28. Beléptetéssel összefüggő adatkezelés	34
29. Munkára képes állapot ellenőrzése	35

A FŐKÉTÜSZ Fővárosi Kéményseprőipari Kft. (a továbbiakban: Társaság) belső adatkezelési folyamatainak nyilvántartása és az érintettek jogainak biztosítása céljából az alábbi Adatvédelmi és adatbiztonsági szabályzatot alkotja.

Társaság neve: **FŐKÉTÜSZ Fővárosi Kéményseprőipari Korlátolt Felelősségű Társaság**
Rövidített neve: **FŐKÉTÜSZ Kft.**
Székhelye: 1145 Budapest, Szugló u. 9-15.
Adószám: 12109584-2-42
Cégjegyzékszám: 01-09-466332
Adatkezelő képviselője: Kovács Balázs Norbert

A Társaság tulajdonosa:

BVH Budapesti Városüzemeltetési Holding Zrt.
1052 Budapest, Városház u. 9-11.
Cg.: 01-10-046833

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

Jelen szabályzatban használt rövidítések:

Infotv. az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény

GDPR vagy

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

Mt. a munka törvénykönyvéről szóló 2012. évi I. törvény

Mvt. a munkavédelemről szóló 1993. évi XCIII. törvény

Ptk. a polgári törvénykönyvről szóló 2013. évi V. törvény

Számv. tv. a számvitelről szóló 2000. évi C. törvény

Szv tv. a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól szóló 2005. évi CXXXIII. törvény

Kstv. a 2015. évi CXXI. törvény a kéményseprő-ipari tevékenységről

Korm. rendelet

99/2016. (V.13.) Korm. rendelet a kéményseprő-ipari tevékenységről szóló törvényvégrehajtásáról

BM rendelet

21/2016. (VI.9.) BM rendelet a kéményseprő-ipari tevékenység ellátásának szakmai szabályairól

NAIH vagy

Hatóság Nemzeti Adatvédelmi és Információszabadság Hatóság

1. A szabályzat célja és hatálya

A Társaság jelen szabályzat megalkotásával és elérhetővé tételével biztosítani kívánja a GDPR 12. cikkében meghatározott megfelelő tájékoztatáson alapuló adatkezelés 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 nevééről, 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 a GDPR 4. cikk 1. pontjában meghatározott személyes adat kezelése megvalósul.

2. Fogalmak

- **Érintett:** azonosított vagy azonosítható természetes személy;
- **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.
- **Különleges adat:**
a faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviseleti szervezeti tagságra, a szexuális életre vonatkozó személyes adat, az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat, valamint a bűnügyi személyes adat.
- **Bűnügyi személyes adat:** a büntetőeljárás során vagy azt megelőzően a bűncselekménnyel vagy a büntetőeljárással összefüggésben, a büntetőeljárás lefolytatására, illetve a bűncselekmények felderítésére jogosult szerveknél, továbbá a büntetés-végrehajtás szervezeténél keletkezett, az érintettel kapcsolatba hozható, valamint a büntetett előéletre vonatkozó személyes adat.
- **Az érintett hozzájárulása:** az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy a megerősített félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok 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, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza; ha az adatkezelés céljait és eszközeit az uniós vagy a tagállami jog határozza meg, az adatkezelőt vagy az adatkezelő kijelölésére vonatkozó különös szempontokat az uniós vagy a tagállami jog is meghatározhatja.
- **Adatkezelés:** a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés.
- **Adattovábbítás:** az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele.
- **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, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel.
- **Adatállomány:** az egy nyilvántartásban kezelt adatok összessége.
- **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:** 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.
- **Adatkezelés korlátozása:** a tárolt személyes adatok megjelölése jövőbeli kezelésük korlátozása céljából.
- **Álnevesítés:** a személyes adatok olyan módon történő kezelése, amelynek következtében további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik, feltéve, hogy az ilyen további információt külön tárolják és technikai, 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 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 helyzetéhez, 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:**
 - az egynél több tagállamban tevékenységi hellyel rendelkező adatkezelő esetében az Unión belüli központi ügyvitelének helye, ha azonban a személyes adatok kezelésének céljaira, eszközeire vonatkozó döntéseket az adatkezelő egy Unión belüli másik tevékenységi helyén hozzák és az utóbbi tevékenységi hely rendelkezik hatáskörrel az említett döntések végrehajtására, az említett döntéseket meghozó tevékenységi helyet kell tevékenységi központnak tekinteni;
 - 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.
- **Felügyeleti hatóság:** egy tagállam által a GDPR 51. cikknek megfelelően létrehozott független közhatalmi szerv.

Amennyiben a mindenkor 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 – és 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 kijelölésre kerül, úgy - az adatvédelmi tisztviselő ellenőrizheti. Amennyiben ilyen személy megbízásra vagy kijelölésre kerül, úgy neve és elérhetősége az 2. sz. mellékletben található.

A Társaság személyes adatot csak az érintett előzetes – különleges személyes adat esetén írásbeli – hozzájárulása vagy törvény, illetve törvényi (rendeleti) 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. A személyes adatokat kezelő és azokhoz hozzáférési lehetőséggel rendelkező személyek kötelesek **Titoktartási nyilatkozatot** tenni (1. sz. melléklet).

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 adatfeldolgozó 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 a GDPR által előírt **Adatfeldolgozó szerződést** köt (minta: 28. sz. melléklet).

4. A Társaság adatvédelmi rendszere

A Társaság vezető tisztségviselője a Társaság sajátosságainak figyelembevételével meghatározza az adatvédelem szervezetét, az adatvédelemre, valamint az azzal összefüggő tevékenységre vonatkozó feladat- és hatásköröket, és 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 kijelölt adatvédelmi tisztviselő útján.

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

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

A Társaság biztosítja az adatvédelmi tisztviselő részére a feladat ellátásához szükséges forrásokat, valamint biztosítja számára, hogy a feladatai ellátása során utasításokat senkitől ne fogadjon el, ezen feladatai ellátásával összefüggésben nem bocsátható el és 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 kijelölt adatvédelmi tisztviselő felett szerződésben meghatározott jogokat a Társaság vezető tisztségviselője gyakorolja.

A vezető tisztségviselő adatvédelemmel kapcsolatos feladatai:

- a) felelős az érintettek GDPR-ban 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.

Az adatvédelmi tisztviselő adatvédelemmel kapcsolatos feladatai:

- a) segítséget nyújt az érintett jogainak biztosításában;
- b) minden év január 15-ig jelentést készít a vezető tisztségviselő részére a Társaság adatvédelmi feladatainak végrehajtásáról;
- c) jogosult jelen szabályzat betartását az egyes szervezeti egységeknél ellenőrizni;
- d) vezeti az adattovábbítási nyilvántartást;
- e) részt vesz a NAIH által szervezett adatvédelmi tisztviselők konferenciáján;
- f) figyelemmel kíséri az adatvédelemmel és információszabadsággal kapcsolatos jogszabályváltozásokat, ezek alapján indokolt esetben kezdeményezi jelen szabályzat módosítását;
- g) közreműködik a NAIH-tól a Társasághoz érkezett megkeresések megválaszolásában és a NAIH által kezdeményezett vizsgálat, illetve adatvédelmi hatósági eljárás során;
- h) általános állásfoglalás megadása céljából megkeresést fogalmaz meg a NAIH felé, amennyiben egy felmerült adatvédelmi kérdés jogértelmezés útján egyértelműen nem válaszolható meg;
- i) tájékoztatást és szakmai tanácsot ad a Társaság adatvédelmi jogszabályokban előírt kötelezettségeinek ellátásával kapcsolatban;
- j) 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;
- k) kérésre szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, valamint nyomon követi a hatásvizsgálat elvégzését;
- l) együttműködik a NAIH-val;
- m) az adatkezeléssel összefüggő ügyekben kapcsolattartó pontként szolgál a NAIH felé, valamint bármely egyéb kérdésben konzultációt folytat le a Hatósággal.

Az informatikáért felelős osztály vezetője (a továbbiakban: Informatikai Osztályvezető) adatvédelemmel kapcsolatos feladatai:

- a) a munkaköre ellátásával kapcsolatosan felmerülő, valamint egyéb szükség szerinti rendszergazdai feladatok ellátása;
- b) ellátja az informatikai fejlesztésekkel, beszerzésekkel kapcsolatos feladatokat, ügyelve a beszerzések racionalizálására, kompatibilitására;
- c) összeállítja az informatikai beszerzések, beruházások, fejlesztések tervezetét;
- d) intézkedési tervet dolgoz ki az adatbiztonsági követelményeknek informatikai szempontból történő megfelelésig biztosítása céljából
- e) szervezi és koordinálja az informatikusok munkáját;
- f) hozzájárulását adja a valamennyi munkavállaló részére a szervereken és adattárolókon található adatok eléréséhez való jogosultsághoz.

Az informatikus adatvédelemmel kapcsolatos feladatai:

- a) ellátja a munkaköri leírásában meghatározott rendszergazdai feladatokat;
- b) a szervezeti egység vezetőjének írásos kérelme alapján közreműködik az adatkezelők egyéni kódjának, jelszavának, jogosultságának beállításában azon szerverek tekintetében, amelyekre adminisztrátori jogosultsággal rendelkezik;
- c) használatba állítás előtt ellátja a szoftverek és hardverek rendszerbe állítását (installálását);
- d) a szervereken tárolt adatok vonatkozásában gondoskodik a kezelt adatok jogosultak általi hozzáféréséről, módosításáról, illetőleg gondoskodik a tárolt adatok megsemmisülésének megakadályozásáról;
- e) igény esetén közreműködik a számítógépen/szerveren tárolt adatok esetében a megadott szempontú adatszolgáltatásban;
- f) elvégzi a szervereken tárolt adatok biztonsági mentését, naplózását;
- g) vírusfertőzöttség esetén elvégzi a fertőzött informatikai eszköz vírusmentesítését, a Társaság Információ Biztonsági Szabályzatában és Szám.tech Szabályzatában leírtak alapján.
- h) szükség szerint ellátja a számítógépek és a hálózat karbantartását, gondoskodik a szerverek üzemszerű működéséről;
- i) ellátja az informatikai eszközök szervizelésével kapcsolatos feladatokat, amennyiben megoldható szakszerviz segítsége nélkül;
- j) üzemzavar esetén elvégzi az informatikai rendszerek újraindítását, a hálózat alkalmazásainak és adatainak a visszatöltését;
- k) folyamatosan üzemelteti a számítógépes hálózatot;
- l) igény esetén segítséget nyújt az adatkezelőknek a számítástechnikai alkalmazások használatánál és az adatbázisok kezelésénél;
- m) minden szakterületét érintő, informatikai szakértelmet kívánó kérdésben segíti az adatvédelmi tisztviselő munkáját.

5. Adatvédelmi incidens kezelése

5.1. 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 Informatikai Osztályvezetőnek is meg kell küldeni.

A bejelentés beérkezését követően az adatvédelmi tisztviselő haladéktalanul megkezdi az adatvédelmi incidens kivizsgálását és értékelését.

5.2. Adatvédelmi incidens kivizsgálása, értékelése

Az adatvédelmi tisztviselő – informatikai rendszert érintő incidens esetén az Informatikai Osztályvezetővel 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, az adatvédelmi incidens egyéb körülményeit, az adatvédelmi incidens által érintett adatok körét, mennyiségét, az adatvédelmi incidenssel érintett személyek körét és számát, az adatvédelmi incidens várható hatásait, az adatvédelmi incidens megelőzésére, következményeinek enyhítésére megtett intézkedések felsorolását.

A bejelentő az adatszolgáltatást haladéktalanul, de legkésőbb 24 órán belül teljesíti az adatvédelmi tisztviselő részére.

Amennyiben az adatvédelmi incidens értékelése vizsgálatot igényel az adatvédelmi tisztviselő az Informatikai Osztályvezetővel, 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 kötelezettségeire, milyen jellegű kockázatról van szó és 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 incidenskezeléshez 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 Informatikai Osztályvezető egyetértésével - dönt.

A vizsgálatot legkésőbb a bejelentésnek az adatvédelmi tisztviselőhöz érkezésétől számított 72 órán belül be kell fejezni és a vizsgálat eredményéről a Társaság vezető tisztviselőjét, valamint a felügyeleti hatóságot az adatvédelmi tisztviselő tájékoztatja.

5.3. 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 incidensnyilvántartás (24. sz. melléklet) pontos vezetéséről, aktualizálásáról az adatvédelmi tisztviselő gondoskodik.

5.4. Az adatvédelmi incidens bejelentése a Hatóság részére

Az adatvédelmi tisztviselő az adatvédelmi incidenst a bekövetkezését követően haladéktalanul, de legkésőbb az incidens bekövetkezésétől 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 adatvédelmi tisztviselő nevét és elérhetőségét,
- az adatvédelmi incidens valószínűsíthető következményeit és
- az adatvédelmi incidens orvoslására és enyhítésére megtett intézkedéseket.

5.5. 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 szabadságára nézve és az érintettek tájékoztatása szükséges, az adatvédelmi tisztviselő haladéktalanul értesíti az érintetteket és erről a Társaság vezető tisztviselőjét is értesíti. Az értesítendő listáját a 25. sz. melléklet tartalmazza.

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 megakadályozzák az adatok 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.

6. Rendszeres tréningek

Az adatvédelmi tisztviselő jelen szabályzatban foglaltak betartása céljából törekszik arra, hogy az adatvédelmi tudatosság növelése céljából adatvédelmi incidensekkel kapcsolatos oktatásra kerüljön sor a munkavállalók részére, amely során a múltban bekövetkezett adatvédelmi incidensek tapasztalatait, vagy a lehetséges adatvédelmi incidensek veszélyeit ismertetik, elemzik, a kockázatok csökkentésével, megelőzésével kapcsolatosan tájékoztatást adnak, illetve az ismereteket ellenőrzik külső szakértők vagy az adatvédelmi tisztviselő maga.

7. 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 egyetlen egy hatásvizsgálat keretében is elvégezhetőek.

A hatásvizsgálatot főszabály szerint az adatvédelmi tisztviselő végzi. Amennyiben nem ő végzi, úgy a Társaság köteles kikérni az adatvédelmi tisztviselő szakmai tanácsát.

A Társaság jelen szabályzat 27. sz. mellékletében leírt szempontrendszer figyelembevételével elvégzi a hatásvizsgálatot.

A hatásvizsgálat elvégzését követően szükség szerint, de legalább az adatkezelési műveletek által jelentett kockázat változása esetén 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 és 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 és el kell különíteni az objektív és szubjektív kockázati elemeket.

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.

8. 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 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 biztosításának védelmében hozott intézkedéseket, garanciákat.

9. Érdekmérlegelés

Az GDPR 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 elvégzi egy érdekmérlegelési tesztet, mely során az adatkezelés céljának szükségességét és az érintettek jogainak és szabadságainak arányos mértékű korlátozását vizsgálja és megfelelően alátámasztja.

Az érdekmérlegelési teszt során 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.

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 a Társaság 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 miatt 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 a Társaság az adott eset sajátos körülményeire tekintettel, ezért a Társaság minden egyes esetben külön érdekmérlegelési tesztet végez el.

Lehetséges forgatókönyv, melytől való eltérés jogát a Társaság fenntartja:

1. lépés: a Társaság 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: a Társaság a jogos érdekét a lehető legpontosabban meghatározza.
3. lépés: a Társaság meghatározza, hogy mi az adatkezelés célja, milyen személyes adatok, meddig tartó adatkezelését igényli a jogos érdek.
4. lépés: a Társaság meghatározza, hogy az érintetteknek mik lehetnek az érdekeik az adott adatkezelés vonatkozásában (például azok a szempontok, amelyeket az érintettek felhozhatnak az adatkezeléssel szemben).
5. lépés: a Társaság elvégzi jogos érdekeinek és az érintettek érdekeinek, alapjogainak súlyozását és ez alapján megállapítja, hogy a személyes adat kezelhető-e. A Társaság meghatározza, hogy miért korlátozza arányosan a Társaság jogos érdeke – és az ennek alapján végzett adatkezelés – a 4. lépésben meghatározott érdekelti jogokat, várakozásokat.
6. lépés: a Társaság meghatározza, mely garanciák biztosíthatják az adatkezelés szükségességét-arányosságát (természetesen más garanciális intézkedések is alkalmazhatók).

A Társaság jelen szabályzat 26. sz. mellékletében leírt szempontrendszer figyelembevételével végzi el az érdekmérlegelést.

10. Adatbiztonsági szabályok

A Társaság adatbiztonsági és informatikai rendszerének hézagmentes, jogszerű, magas szintű védelmet biztosító szabályozási struktúrájának kialakítása folyamatban van. Ennek keretében a Informatikai Osztályvezető az egyes érintett szervezeti egységek támogatásával, a vezető tisztségviselő jóváhagyásával részletes intézkedési terv(ek)et dolgoz ki és hajt végre. Ennek keretében kerül sor különösen a Társaság

Információ Biztonsági Szabályzatának valamint Szám.tech. Szabályzatának revíziójára/megalkotására, továbbá az adatbiztonsági szint emelését szolgáló beruházások eszközölésére, illetőleg a jelen pontban leírtak folyamatos betartására.

Szerverek

A Társaság által működtetett szerverek saját szerverek.

A kritikus rendszereket futtató központi rendszer esetén, biztonsági mentés történik. Távoli hozzáférés csak VPN-en keresztül lehetséges. Továbbá irányadóak, a Társaság saját, belső szabályzatai is.

Szerverszoba

A székhelyen található a szerverszoba. A helyiség kulccsal vagy mágneskártyás beléptető rendszerrel és elektronikus megfigyelőrendszerrel ellátott. A jogosult személyek listája ellenőrzésre kerül az IT és a vezetés által.

A Társaság saját honlapjai

www.kemenysepro.hu (közszolgáltatás), valamint a www.kemenysepro.info (piaci szolgáltatás), amelyeket a Társaság maga kezel. A honlapok cookie-kat használnak, amelyről a Társaság főoldalán található információk. A honlapra feltöltendő tájékoztató jelen szabályzat 20. sz. melléklete.

Szoftverek telepítéséhez rendszergazdai jogosultság szükséges.

Főszabály szerint az internet használata nem megengedett. Ez alól mentességet élvez a vezetés és azok, akik kérelem alapján engedélyt kaptak használatára. A céges eszközökön csak az IT rendelkezik admin. joggal, így az alkalmazások telepítése ellenőrzött, a felhasználó által nem lehetséges. A magánjellegű file-ok tárolása nem megengedett.

10.1. 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 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. A megsemmisítésről jelen szabályzat 23. sz. mellékletét kell kitölteni.

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

10.2. 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 Társaság;

- 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;
- 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 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, a mentés a központi szerver teljes adatállományára vonatkozik, és mágneses adathordozóra történik;
- a lementett adatokat tároló mágneses adathordozó az erre a célra kialakított páncéldobozban tűzbiztos helyen és módon tárolt;
- a személyes adatokat kezelő hálózaton a vírusvédelemről folyamatosan gondoskodik;
- a rendelkezésre álló számítástechnikai eszközökkel, azok alkalmazásával megakadályozza illetéktelen személyek hálózati hozzáférését.

10.3. Szerverek biztonsága

A Társaság által kezelt személyes adatok áramlását elektronikus módon szerverek segítségével, fizikai tárolásukat pedig adattárolók segítségével valósítják meg. Mind az adattárolókat, mind pedig a szervereket külön erre a célra kialakított helyiségben kell elhelyezni. Erre a helyiségre vonatkozóan ki kell alakítani egy hozzáférési jogosultsággal rendelkező munkavállalói bázist, akik engedéllyel férhetnek hozzá ezekhez az eszközökhöz és esetlegesen a rajtuk tárolt adatokhoz. A szerverszobába való belépési jogosultságot a munkavállalónak külön kell igényelnie, amit az Informatikai Osztályvezetőnek - az adatvédelmi tisztviselővel egyeztetve- kell elbírálnia.

A helyiségbe csak jelen szabályzat 17. sz. mellékletében meghatározott és tételesen felsorolt személyek léphetnek be.

A személyes adatok tárolásának helyén, a szerverszobákban tárolt szerverek fizikai védelme érdekében a Társaság az alábbi intézkedéseket és garanciális elemeket alkalmazza:

- a szerverszoba fizikai védelmét elektronikus megfigyelőrendszerek biztosítják,
- a szerverszoba klimatizált és tűzjelző berendezéssel ellátott,
- a szerverszobába csak a szerverszoba kulcsfelvételi engedéllyel (16. sz. melléklet) rendelkező személy rendelkezhet saját kulccsal vagy veheti át a kulcskezelési szabályok alapján a kulcskezelőtől a szerverszoba kulcsát,
- a kulcsfelvételi engedéllyel rendelkezőkről nyilvántartást vezet az Adatkezelő,
- a kezelt kulcsok típusa lehet állandó vagy eseti, állandó kulcsfelvételi jogosultság birtokában dedikált kulccsal rendelkezhet az engedély birtokosa,
- a Társaság ezen feladattal megbízott munkatársa a kulcskezelési szabályok alapján folyamatosan rögzíti a nem dedikált kulcsok felvételét és leadását,
- amennyiben olyan személynek kell tevékenysége ellátása miatt bemenni a szerverszobába, aki nem jogosult a kulcs felvételére vagy nem a Társaság alkalmazottja, akkor minden esetben tartózkodik vele egy olyan személy is a szerverszobában, aki kulcsfelvételi engedéllyel rendelkezik.

11. 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 naprakészége nagymértékben hozzásegíti a Társaságot a tőle elvárt, illetve általa elérhető biztonsági szint teljesítéséhez. A szabályozás kiterjed az elektronikus megfigyelőrendszerek informatikai rendszerére és az azokhoz csatlakozó eszközökre.

Az informatikai rendszerben a jogosultságok változásait (létező jogosultságok, új jogosultságok kiosztása, módosítása, megszüntése) 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 Informatikai Osztályvezető 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. A nem nevesített rendszergazdai jelszavakat zárt borítékban, felbontást gátló módon, aláírva kell tárolni. Ezek használatát az Adatkezelő vezető tisztségviselője vagy akadályoztatása esetén helyettesítési rend szerinti helyettese engedélyezheti. A nem nevesített felhasználói jogosultságok használatát indokolni és dokumentálni kell.

11.1. Jogosultságkezelési folyamat

Jogosultságigényléshez, - módosításhoz az IT-vezetőnek címzett, jelen szabályzat 21. sz. mellékletét képező, aláírt „Jogosultságkezelési megrendelőlap”-ot kell küldeni. A megrendelőlapot papíralapon vagy elektronikus formátumban, az aláírt példányt beszkenelve kell eljuttatni az Informatikai Osztályvezetőnek.

A jogosultság kezelésekről az Informatikai Osztályvezető belső nyilvántartást vezet, amely a szabályzat 22. sz. melléklete.

Az Informatikai Osztályvezető minden esetben konzultál a megrendelőlapon szereplő jogosultság megadásáról vagy módosításáról annak indoklásának tekintetében a jogosultság birtokosával és az igénylő feletti munkáltatói jog gyakorlójával. A jogosultság megadásával vagy módosításával kapcsolatosan a vezető tisztségviselőnek vétőjoga van.

A megszületett döntést követően az Informatikai Osztályvezető által kijelölt munkatárs beállítja a jogosultságokat, amellyről visszaigazolást küld az igénylő felé.

A jogosultság birtokosának munka- vagy egyéb jogviszonya megszűnésével közvetlen felettesének kötelessége értesíteni az Informatikai Osztályvezetőt, valamint a munkáltatói jogok gyakorlóját a jogosult eddig birtokolt jogosultságainak törlése érdekében. Ebben az esetben a kilépő munkavállaló az informatikai munkaeszközöket (különösen az adathordozásra alkalmas eszközöket) az Informatikai Osztályra átadja adatmentésre és átvilágításra.

A jogosultság megszüntése esetén a jogosult felettese a megszüntetési kérelmet elektronikus módon vagy papíralapon a jogosultságkezelési megrendelőlapon küldi meg az Informatikai Osztályvezetőnek, aki gondoskodik a jogosultság törléséről. Ezt követően az Informatikai Osztályvezető vagy az általa megbízott munkatárs visszajelzést küld a törlést kezdeményezőnek.

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

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

12. 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, és

technikai és szervezési intézkedések megtételével biztosítja, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet kapcsolni.

Az álneven történő adatkezelést a Társaság a nagyobb fokú biztonság érdekében, valamint a statisztikai célra gyűjtendő adatok vagy a fejlesztés, tesztelés, karbantartás alatt álló rendszerek esetében 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 és továbbfejlesztesse azokat.

13. Beépített adatvédelem

Bevezetésre került az ún. beépített adatvédelem (*privacy by design*), melynek következtében a Társaság már az adatkezelés tényleges megkezdése előtt – például már a projektelőkészítés időszakában – is figyelemmel volt 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 és továbbfejlesztesse azokat. Az adatkezelésnek átláthatónak és felhasználó-központúnak, az adatvédelemnek proaktívnak kell lennie, és az adat teljes életciklusát fel kell ölelnie, vagyis a teljes folyamatnak része kell, hogy legyen.

A Társaság 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, mind az adatkezelés módjának meghatározásakor, mind pedig az adatkezelés során olyan megfelelő technikai és szervezési intézkedéseket –

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

- hajt végre, amelyek célja egyrészt az adatvédelmi elvek, például az adattakarékosság hatékony megvalósítása, másrészt a GDPR-ben foglalt követelmények teljesítéséhez és az érintettek jogainak védelméhez szükséges garanciák beépítése az adatkezelés folyamatába.

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. Ezek az intézkedések különösen azt kell, hogy biztosítsák, hogy a személyes adatok alapértelmezés szerint a 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 előbbieken előírt követelményeket.

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

A beépített és az alapértelmezett adatvédelem elveit a közbeszerzések, beszerzések és egyéb jellegű szerződéskötések 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, és 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 és 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.

14. Mobil eszköz menedzsment

Az adatvédelmi szabályozás szempontjából a mobil eszköz menedzsment területén a Társaság üzletmenetéhez fontos szolgáltatások, műszaki technikai, informatikai biztosítása mellett adatvédelmi szempontból fontos kötelezettség keletkezik, azaz biztosítani kell a Társaság birtokába kerülő adatok titkosságát, sérthetetlenségét és a biztonságot garantáló keretrendszerben való működését.

Mobil eszköznek kell tekinteni: minden olyan hordozható, elektronikus eszköz, mely rendelkezik az alábbi tulajdonságokkal:

- Akkumulátorról üzemel
- Támogat valamilyen vezeték nélküli technológiát
- Rendelkezik valamilyen felhasználói felülettel (pl. gombjai vannak), „ember által kezelhető”
- Korlátozott képességű hardverrel rendelkezik.

Így különösen: mobiltelefon, laptop, tablet, GPS berendezés

A Társaság rendszerében mobilmenedzsment szolgáltatások biztosítása során kiemelet figyelmet fordít a személyes adatok védelmére és az egyes mobileszközök informatikai védelmére, adatvédelmi incidensek megelőzésére. Ennek céljából a mobil eszköz menedzsment részét képezi:

- összetett és rendszeresen változó jelszóhasználat kikényszerítése az alkalmazott szoftverek esetében,
- VPN titkosítás használata a rendszerben levő eszközökön,
- mobiltelefonok távoli letiltása,
- számítógépek távoli ellenőrzése,

- nyomkövetés és helymeghatározási opció távoli bekapcsolásának lehetősége (GPS berendezések céges gépjárművekben).

15. Oktatás és tréningrendszer

Kiemelt területként kell kezelni a munkavállalók kapcsán a biztonságtudatossági képzést a szervezet informatikai és nem informatikai alkalmazottai részére, tekintettel a Társaság gazdasági erőforrásaira és munkaszervezési szempontokra.

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 ajánlott 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 bírságból eredő károkon túl a pénzügyi eredményekben is nyilvánvalóan megmutatkozik.

16. Az érintettek jogainak érvényesítése

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

Az érintett jogosult arra, hogy a rá vonatkozó, általa az Adatkezelő rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel 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.

Az érintett kérelmére az Adatkezelő tájékoztatást ad az érintett általa kezelt, illetve az általa vagy rendelkezése szerint megbízott adatfeldolgozó által feldolgozott adatairól, azok forrásáról, az adatkezelés céljáról, jogalapjáról, időtartamáról, az adatfeldolgozó nevéről, címéről és az adatkezeléssel összefüggő tevékenységéről, az adatvédelmi incidens körülményeiről, hatásairól és az elhárítására megtett intézkedésekről, továbbá - az érintett személyes adatainak továbbítása esetén - az adattovábbítás jogalapjáról és címzettjéről.

A tájékoztatás főszabály szerint ingyenes, ha a tájékoztatást kérő a folyó évben azonos adatkörre vonatkozóan tájékoztatási kérelmet az Adatkezelőhöz még nem nyújtott be. Egyéb esetekben költségtérítés állapítható meg. A költségtérítés mértékét a felek között létrejött szerződés is rögzítheti. A már megfizetett költségtérítést vissza kell téríteni, ha az adatokat jogellenesen kezelték, vagy a tájékoztatás kérése helyesbítéshez vezetett.

A valóságnak nem megfelelő adatot az adatot kezelő szervezeti egység vezetője – amennyiben a szükséges adatok és az azokat bizonyító közokiratok rendelkezésre állnak – helyesbíti, a GDPR. 17. cikkében meghatározott okok fennállása esetén intézkedik a kezelt személyes adat törléséről.

A személyes adatot törölni kell, ha

- 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) az érintett tiltakozik az adatkezelés ellen, és nincs elsőbbséget élvező jogszerű ok az adatkezelésre, vagy az érintett tiltakozik az adatkezelés ellen;
- d) a személyes adatokat jogellenesen kezelték;
- e) a személyes adatokat az adatkezelőre alkalmazandó uniós vagy tagállami jogban előírt jogi kötelezettség teljesítéséhez törölni kell;
- f) a személyes adatok gyűjtésére a 16 éven aluli gyermekek részére az információs társadalommal összefüggő szolgáltatások kínálásával kapcsolatosan került sor.
- g) ha az adatkezelő nyilvánosságra hozta a személyes adatot, és a személyes adatokra már nincs szükség abból a célból, amelyből azokat gyűjtötték vagy más módon kezelték úgy azt törölni köteles, valamint 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.

Az érintett tiltakozhat személyes adatának kezelése ellen,

- ha a személyes adatok kezelése vagy továbbítása kizárólag az Adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez vagy az Adatkezelő, adatátvevő vagy harmadik személy jogos érdekének érvényesítéséhez szükséges, kivéve kötelező adatkezelés esetén;
- ha a személyes adat felhasználása vagy továbbítása közvetlen üzletszerzés, közvélemény-kutatás vagy tudományos kutatás céljára történik; valamint
- törvényben meghatározott egyéb esetben.

Az Adatkezelő a tiltakozást a kérelem benyújtásától számított legrövidebb időn belül, de legfeljebb 15 napon belül megvizsgálja, annak megalapozottsága kérdésében döntést hoz, és döntéséről a kérelmezőt írásban tájékoztatja.

Ha az Adatkezelő az érintett tiltakozásának megalapozottságát megállapítja, az adatkezelést - beleértve a további adatfelvételt és adattovábbítást is – megszünteti, az adatokat zárolja, valamint a tiltakozásról, továbbá az annak alapján tett intézkedésekről értesíti mindazokat, akik részére a tiltakozással érintett személyes adatot korábban továbbította és akik kötelesek intézkedni a tiltakozási jog érvényesítése érdekében.

Ha az érintett az Adatkezelő döntésével nem ért egyet, illetve, ha az Adatkezelő a válaszadási határidőt elmulasztja, az érintett - a döntés közlésétől, illetve a határidő utolsó napjától számított 30 napon belül - bírósághoz fordulhat.

Ha az adatátvevő jogának érvényesítéséhez szükséges adatokat az érintett tiltakozása miatt nem kapja meg, úgy az értesítés közlésétől számított 15 napon belül, az adatokhoz való hozzájutás érdekében bírósághoz fordulhat az Adatkezelő ellen. Az Adatkezelő az érintettet is perbe hívhatja.

Ha az Adatkezelő az értesítést elmulasztja, az adatátvevő felvilágosítást kérhet az adatátadás megghiúsulásával kapcsolatos körülményekről az Adatkezelőtől, amely felvilágosítást az Adatkezelő az adatátvevő erre irányuló kérelmének kézbesítését követő 8 napon belül köteles megadni. Felvilágosítás kérése esetén az adatátvevő a felvilágosítás megadásától, de legkésőbb az arra nyitva álló határidőtől számított 15 napon belül fordulhat bírósághoz az Adatkezelő ellen. Az Adatkezelő az érintettet is perbe hívhatja.

Az Adatkezelő az érintett adatát nem törölheti, ha az adatkezelést törvény rendelte el. Az adat azonban nem továbbítható az adatátvevő részére, ha az Adatkezelő egyetértett a tiltakozással, vagy a bíróság a tiltakozás jogosságát megállapította.

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 kérhet 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 jogorvoslati lehetőséggel, panasszal a Nemzeti Adatvédelmi és Információszabadság Hatóságnál (1125 Budapest, Szilágyi Erzsébet fasor 22/C.), illetve lakóhelye vagy tartózkodási helye szerint illetékes törvényszéknél élhet.

17. A Társaságnál megvalósuló adatkezelések

Az adatkezelés helye: 1145 Budapest, Szugló utca 9-15.

Társaság székhelye: 1145 Budapest, Szugló utca 9-15.

Az egyes adatkezelésekhez kapcsolódó adatfeldolgozók és az esetleges adattovábbítások címzettjei a jelen Szabályzat 3.sz. mellékletében kerültek feltüntetésre. Az adatfeldolgozást végző partnerekkel a Társaság minden esetben külön adatfeldolgozói szerződést köt a megvalósuló adatkezelés részleteire specializáltan.

Az adatkezelések nyilvántartási számai:

A GDPR alkalmazásával egyidejűleg a NAIH adatkezelési folyamatok nyilvántartása megszűnik, helyét az adatkezelő saját szervezetén belüli nyilvántartásvezetési kötelezettsége váltja fel (GDPR 30. cikk).

18. Közszolgáltatási tevékenységgel összefüggő adatkezelések

A FŐKÉTÜSZ Fővárosi Kéményseprőipari Kft. Budapest kéményseprő-ipari közszolgáltatója. A szolgáltatás profilja a kéményseprő-ipari közszolgáltatásról szóló 2015. évi CCXI. törvény, a 21/2016. (VI.9.) BM rendelet a kéményseprő-ipari tevékenység ellátásának szakmai szabályairól, valamint a 99/2016. (V.13.) Korm. rendelet a kéményseprő-ipari tevékenységről szóló törvény végrehajtásáról összhangban a következők:

- a lakó- és középületekben üzemelő tüzelőberendezések kéményeinek időszakos ellenőrzése és szükség szerinti tisztítása,
- a műszeres és hagyományos kéményvizsgálatok végzése, nyilatkozatok készítése,
- kémények és tartozékaik műszaki felülvizsgálata,
- hatósági eljárásokhoz kapcsolódó feladatok ellátása

A FŐKÉTÜSZ Kft. és Budapest Főváros Önkormányzata között 2014.04.01-től fennálló Közszolgáltatási Szerződés, valamint annak későbbi módosítása alapján a főváros egész területén kizárólagos joggal végzi a kéményseprő-ipari közszolgáltatást.

adatkezelés célja: közüzemi szolgáltatás nyújtása, a kötelező kéményseprő-ipari közszolgáltatás ellátása

kezelt adatok köre: szolgáltatás alatt köteles megadni: családi és utónév, cím, tartózkodási cím, ingatlan címadatai, gazdálkodási szervezet: név, székhely, fióktelep, képviselő neve, cégjegyzékszám vagy egyéb nyilvántartási szám

adatkezelés jogalapja: a kéményseprő-ipari közszolgáltatásról szóló 2015. évi CCXI. törvény 5.§ b), valamint a Főváros Önkormányzatával kötött és 2014.04.01-jétől hatályos Közszolgáltatási Szerződés, valamint a GDPR 6. cikk (1) a) - e)

adattárolás határideje: általános elévülésig

adattárolás módja: papírlapon és elektronikusan

Az ügyfeleknek történő számlázás esetében külső céget vehet igénybe a Társaság, ez a cég jelen adatkezelési folyamat során adatfeldolgozónak minősül.

19. Ügyfélszolgálati tevékenységgel összefüggő adatkezelés

Amennyiben valaki panasszal kíván élni az Adatkezelő irányában, azt megteheti **személyesen** (1145 Budapest, Szugló u. 9-15.), **telefonon** (+1-999-06-64), **írásban postai úton** (1443 Budapest, Pf. 155.) vagy **elektronikusan** (adatvedelem@kemenysepro.hu).

Ügyfél panaszok esetében jegyzőkönyvet vesznek fel. Ilyen esetben, ha az érintett a panasz kezelésével nem ért egyet, vagy annak azonnali kivizsgálása nem lehetséges, a panaszról jegyzőkönyvet készítenek, amelynek egy másolati példányát a Társaságnak át kell adnia a panaszosnak.

A panaszról felvett jegyzőkönyv az alábbiakat kell tartalmazza:

- a) a panaszos neve;
- b) a panaszos lakcíme, székhelye, illetve amennyiben szükséges, levelezési címe;
- c) a panasz előterjesztésének helye, ideje, módja;
- d) a panaszos panaszának részletes leírása, a panasszal érintett kifogások elkülönítetten történő rögzítésével, annak érdekében, hogy a fogyasztó/vevő panaszában foglalt valamennyi kifogás teljes körűen kivizsgálásra kerüljön;
- e) a panasszal érintett szerződés száma (ha van);
- f) a panaszos által bemutatott iratok, dokumentumok és egyéb bizonyítékok jegyzéke;
- g) a jegyzőkönyvet felvevő személy és a panaszos aláírása (utóbbi formai elem személyesen közölt szóbeli panasz esetén elvárt);
- h) a jegyzőkönyv felvételének helye, ideje.

adatkezelés célja: panaszok felvétele, szolgáltatási tevékenységgel összefüggő panaszkezelés intézése

kezelt adatok köre:

panaszos neve, címe, telefonszáma, e-mail címe, a panasz tárgya, a panasz érkezésének időpontja jogi személy esetén: panaszos vevő neve, székhelye, adószáma, telefonszáma, e-mail címe, a panasz tárgya, a panasz érkezésének időpontja

adatkezelés jogalapja: GDPR 6. cikk (1) a) szerinti; a fogyasztóvédelemről szóló 1997. évi CLV. törvény 17/A. § (6)-(7) bekezdése

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

adattárolás módja: papíralapú és elektronikus

A telefonon történt bejelentések esetében a beszélgetések rögzítésre kerülnek. A telefonos hangrögzítés adatkezelésével kapcsolatos főbb ismérvek az alábbiak:

adatkezelés célja: a beérkező panaszok, kérelmek megválaszolásához szükséges elérhetőségek rögzítése, a panaszok, hibabejelentések felvétele.

kezelt adatok köre: érintett hangja, általa megadott adatok

adatkezelés jogalapja:

törvényi felhatalmazás (a fogyasztóvédelemről szóló 1997. évi CLV. törvény 17/B. § (3)); érintett beleegyezése (GDPR 6. cikk (1) a))

adatkezelés időtartama: az adatrögzítéstől számított 5 év

adattárolás módja: elektronikusan

A telefonos hangrögzítésről részletes adatvédelmi tájékoztató készült, amely jelen Szabályzat 19. sz. melléklete

20. Hátralékkezelés

Fizetési hátralék esetén első lépésben Fizetési emlékeztető kerül megküldésre az ügyfél részére nem könyvelt postai küldeményként, mely tartalmazza a hátralékos számlák részletes felsorolását.

Amennyiben a Fizetési emlékeztetőben megadott határnapig a tartozás nem kerül rendezésre, úgy következő lépésként Fizetési felszólítás kerül kiküldésre a hátralék ismételt számlánkénti részletezésével tértivevényes postai küldeményként. A Fizetési felszólítás már tartalmazza a nem fizetés jogkövetkezményeinek ismertetését.

Az eredménytelen felszólításokat követően - a várható eredményesség mérlegelése alapján - behajtási eljárást kezdeményez a Társaság, amely fizetési meghagyási szakaszból és szükség esetén végrehajtási/peres szakaszból áll.

A hátralékosok adatai továbbításra kerülhetnek külsős ügyvédi iroda – és végső esetben a hatáskörrel és illetékességgel rendelkező bíróság - felé.

adatkezelés célja: Adatkezelő szolgáltatási területén az ügyfeladatok kezelése hátralékkezelés céljából

kezelt adatok köre: név, leánykori név, anyja neve, születési hely, születési idő, állandó lakhely, telefonszám, levelezési cím, e-mail cím

adatkezelés jogalapja: a GDPR 6. cikk (1) f) szerinti jogos társasági érdek érvényesítése és a 2009. évi L. törvény 20. § (1) szerinti felhatalmazás

adattárolás határideje: a hátralék kiegyenlítése, vagy a hátralékkal kapcsolatos polgári jogi igények elévülése (5 év)

adattárolás módja: elektronikus és papíralapon

21. Piaci szolgáltatásokkal kapcsolatos adatkezelések

21.1. Nem lakossági szektornak történő szolgáltatás

A Társaság a kéményseprő-ipari tevékenységről szóló 2015. évi CCXI. törvény rendelkezéseinek megfelelően 2016. július 1-jétől Budapest közigazgatási területén kívül, meghatározott megyékben egyedi megrendelés alapján kéményseprő-ipari szolgáltatóként végzi a nem lakossági szektor kéményellenőrzését, illetve minden egyéb kéményseprő-ipari tevékenységhez kapcsolódó szolgáltatást, amelyre a jogszabály lehetőséget biztosít számára.

Ezen tevékenysége során a Társaság személyes adatot csak igen kis számban kezel, hiszen ilyen lehet pl.: a jogi személyek, társasházak, lakásszövetkezet természetes személy kapcsolattartójának adatai. A Társaság kijelenti, hogy amennyiben az ilyen jellegű piaci szolgáltatása során személyes adatok kezelésére kerülne sor, úgy azt a Társaság a jelen szabályzatban meghatározottak szerint kezeli és azokra a jelen szabályzatban és a vonatkozó jogszabályokban előírt rendelkezések vonatkoznak.

22. Webshop üzemeltetés

A Társaság az alábbi weboldalon: <http://kemenysepro.hu/szolgáltatások/piaci-szolgáltatások/webaruhaz/> elektronikus kereskedelmi szolgáltatást üzemeltet, amely szolgáltatás kizárólag Magyarország közigazgatási határain belül érhető el.

Az elektronikus kereskedelmi tevékenységgel kapcsolatos adatkezelésekről a fent hivatkozott felületen elérhető ÁSZF és Adatvédelmi tájékoztató rendelkezik azzal, hogy az abban nem szabályozott adatkezelések tekintetében a jelen Szabályzat és a vonatkozó magyar jogszabályok az irányadók.

23. Személyügyi adatkezelések

23.1. A Társasághoz történő jelentkezés folyamata

A Társasághoz érkehetnek jelentkezések álláshirdetésen keresztül, közvetlen jelentkezéssel, valamint ajánlás útján, illetve speciális tudást igénylő munkapozíciók esetében ún. 'fejvadász cégeken' keresztül is.

23.2. Fejvadász cégen keresztül érkező jelentkezés:

'Fejvadász' cégen keresztül jelentkező személyek esetében a 'fejvadász' cég kezeli a jelentkező önéletrajzát, és a jelentkező a 'fejvadász' cég előszűrését, majd a Társaság interjúját követően lesz/nem lesz munkavállalója a Társaságnak.

23.3. Hirdetésen keresztül történő jelentkezés:

A hirdetések többféle úton kerülnek feladásra (újság, online stb.). Az álláskeresők vagy a megadott e-mail címre vagy személyesen tudják eljuttatni az önéletrajzukat. Több lépcsős eljárást követően a Társaság dönti el, hogy alkalmazza-e a jelentkezőt.

23.4. A nem meghirdetett álláshelyre való jelentkezéssel és a munkaerő-toborzással kapcsolatos közös szabályok

A Társaság a munkára jelentkezés céljából érkezett személyes adatokat tartalmazó önéletrajzok (továbbiakban: CV) esetén nem tesz különbséget azok érkezésének módja között: azonos elbírálás alá esik a papíralapon és az elektronikus módon érkezett CV.

Főszabály szerint az önéletrajzokat későbbi felhasználás céljából tárolja a Társaság, adatbázist nem épít belőlük. A CV-ket max. egy évig tárolja a Társaság papírlapon az interjúján részt vett pályázók anyagával.

Minden, a Társaság előtt feltárt CV esetében az adatkezelésre a GDPR 6. cikk (1) a) pontja ad jogalapot.

Az adatkezeléshez adott hozzájárulás megdönthető, így az érintett jelen szabályzat szerint meghatározottak alapján visszavonhatja hozzájárulását.

23.5. A nem meghirdetett álláshelyre való jelentkezésre vonatkozó különös szabályok

A nem meghirdetett álláshelyre való jelentkezés esetén a Társaság válaszlevelet küld a jelentkezőnek, amelyben tájékoztatja az adatkezelés tényéről, jogalapjáról és az adatkezelés elleni tiltakozás formáiról. A „Válaszlevél önéletrajzokra” című válasz a szabályzat 4. sz. melléklete. A nem meghirdetett álláshelyekre érkező önéletrajzokat a Társaság értékelést követően törli.

23.6. Az ajánlás útján érkező önéletrajzokra vonatkozó különös szabályok

A Társaság ismeri és elismeri a munkavállalói ajánlás rendszerét. A Társaság bármely munkavállalója ajánlhatja ismerősét általánosságban vagy egy konkrét pozícióra – ebben az esetben azonban az ajánló munkavállaló felelős az általa átadott személyes adatok jogszerű felvételéért, kezeléséért és átadásáért. Ebben az esetben a Társaság az érintett hozzájárulását csak vélelmezni tudja, így a Társaság mindent megtesz azért, hogy érintetti tiltakozás esetén tájékoztassa az érintetteket jogainak érvényesítésének lehetőségeiről és az adatkezelés elleni tiltakozás formáiról. Jogalap nélküli adatátadás esetén pedig a Társaság intézkedik a kezelt adatok azonnali törlése felől.

adatkezelés célja: a megüresedő álláshelyek betöltésére a munkaviszony későbbi létesítése céljából, megfelelő leendő munkavállaló kiválasztása

kezelt adatok köre: név, születési dátum, anyja neve, lakcím, képzési adatok, fénykép, az érintett által megadott egyéb adatok, ajánló személyazonosító adatai, háttérellenőrzés sikerességének ténye

adatkezelés jogalapja: a GDPR 6. cikk (1) a)

adattárolás határideje: az érintett törlési kérelméig, maximum 1 év

adattárolás módja: papíralapon és elektronikusan

24. Munkaviszonnal kapcsolatos adatkezelés

A munkaviszonnal kapcsolatos adatkezelés célja a munkaviszony létesítése, fenntartása és megszüntetése.

A Társaság jogszabályi előírás vagy egyéb jogviszony teljesítésének okán fenntartja magának a jogot, hogy olyan munkavállalót alkalmazzon, aki erkölcsileg megfelel az elvárásainak, ezért a Társaság a felvételt tiszta erkölcsi bizonyítvány meglétéhez köti, amelyre a jogalapot a 2015. évi CXXI. törvény 4.§ (2) adja.

A tiszta erkölcsi bizonyítvány ellenőrzését a humánpolitikáért felelős szervezeti egység vezetője végzi, ő ellenőrzi az erkölcsi bizonyítványt:

- érvényességét (bárki számára elérhető módon), illetve
- annak tartalmát.

A Társaság bűnügyi személyes adatot csak az érintett írásbeli hozzájárulásával kezel. A Társaság előzetesen tájékoztatja az érintettet, hogy a bűnügyi személyes adat kezelésének célja az adott munkakörre való érdemesség eldöntése és jogszabályi előírás betartása, így ezen adatot csak a cél megvalósulásáig, a döntésig kezeli.

A Társaság csak az adott, konkrét munkakör feltételeként köti ki a büntetlen előéletet. Egyes méltányolható esetekben azonban a Társaság vezető tisztségviselője, egyedi elbírálás során, dönthet a munkakörre való alkalmasság megítélése mellett akkor is, ha olyan bejegyzés található az erkölcsi bizonyítványban, amely

- a bírósági mentesíthetőség időszakában tart,
- a törvényi mentesítési idő beálltához közel van,

A munkára való jelentkezés során az adatok az alábbiak alapján a döntési jogkörrel rendelkező személyhez kerülnek. A munkakörre való alkalmasság elbírálása ugyanis minden esetben a szakmai vezetők jogköre. A munkára jelentkezés során megadott adatokat így csak a Humánpolitikai Osztály vezetője (felhatalmazásával a Humánpolitikai Osztály munkavállalója) és a fent ismertetett különleges esetekben a Társaság vezető tisztségviselője ismerhetik meg.

Az adatokhoz az itt megjelölteken kívül senki sem férhet hozzá, így a Társaság más munkavállalója vagy egyéb, a Társasággal más jogviszonyban álló személy azokat semmilyen módon és formában nem ismerheti meg.

Az érintett meghatározott munkakörre vonatkozó munkaviszony létesítése során megkéri érvényes erkölcsi bizonyítványát is. A Társaság minden esetben keresi a lehető legjobb módszert arra, hogy ne korlátozza az érintett magánszféráját, s mivel egy érvényes erkölcsi bizonyítvány a kiállításától számított 90 napon belül felhasználható a Társasághoz történő jelentkezésen kívüli más célokra is, ezért a Társaság nem iktatja be az érintett erkölcsi bizonyítványt fizikailag.

Azért, hogy az azon szereplő adatot csak az illetékes személy ismerhesse meg, a Társaság kötelezően kiköti, hogy a felvételi eljárás során az erkölcsi bizonyítványt az érintett csak a szakmai vezető, a humánpolitikáért felelős szervezeti egység vezetője, illetve a jelen pontban meghatározott különleges esetekben a Társaság vezető tisztségviselője előtt tárhatja fel.

Amennyiben különleges méltánylást igénylő esetben a munkaviszony létesítésével kapcsolatos eljárás során az érintett nem tud erkölcsi bizonyítványt bemutatni, úgy azt postán is megküldheti hiánypótlásként a Társaságnak. Ebben az esetben 30 napos határidőn belül;

- a vezető tisztségviselő dönt a munkaviszonyról,
- a dokumentum a döntési eljárás zárultával postai úton, utólag is nyomon követhető módon visszaküldésre kerül az érintettnek.

Annak érdekében, hogy a Társaság bizonyítani tudja, hogy

- a felvételi eljárás során megvizsgálta az erkölcsi bizonyítvány érvényességét,
- a felvételi eljárás során milyen elérhető adatok alapján ítélte meg a leendő munkavállalót, az alábbi adatokat a munkaviszony fenntartásához szükséges adatokkal együtt, azonos tárolási módon és tárolási határidővel rögzíti:
 - erkölcsi bizonyítvány kiállításának dátuma
 - erkölcsi bizonyítvány okmányszáma
 - erkölcsi bizonyítvány kérelem azonosítója

Ezen adatok a törvény szerint azonban nem számítanak különleges személyes adatnak, mert nem bűnügyi személyes adatok. Ezen adatok alapján a Belügyminisztérium Nyilvántartások Vezetéséért Felelős Helyettes Államtitkárság rendszerében utólag minden, 2013. január 1.-je után kiállított erkölcsi bizonyítvány valóságos és tartalma ellenőrizhető.

A Társaság így sem a felvételi eljárás során, sem a munkaviszony kapcsán nem tárol erkölcsi bizonyítványt, sem az erkölcsi bizonyítványról való bármilyen másolatot.

Abban az esetben, ha a munkára jelentkező érintett nem kerül kiválasztásra, úgy az ő adatait, azaz az erkölcsi bizonyítvánnyal kapcsolatos adatait a Társaság haladéktalanul törli a kiválasztási folyamat végeztével.

Amennyiben a jövőben olyan munkakörre történő jelentkezéshez használja fel Társaság az érintett adatait, ahol az érintettnek tiszta erkölcsi bizonyítványra van szüksége, úgy az érintettet ismét egy érvényes erkölcsi bizonyítvány bemutatására kérheti fel.

24.1. Munkakör betöltéséhez szükséges orvosi alkalmassági vizsgálat

A Társaságnál a már munkavállalói státuszúaknak a foglalkozási osztályba sorolásuktól függő gyakorisággal orvosi alkalmassági vizsgálaton kell megjelenniük. Az orvosi vizsgálatot a Társaság megbízási szerződéssel működő foglalkozás-egészségügyi orvos végzi. A vizsgálat eredményét a Társaság nem ismeri meg, az az orvostól marad, a Társasághoz csak az alkalmas/nem alkalmas minősítés jut el.

A munkaköri, szakmai, illetve személyi higiénés alkalmasság orvosi vizsgálatáról és véleményezéséről szóló 33/1998. (VI. 24.) NM rendelet hatálya kiterjed a Társaságra, mint a munkavédelemről szóló 1993. évi XCIII. törvény 87. § 9. pontja szerinti szervezett munkavégzés (a továbbiakban: szervezett munkavégzés) keretében munkavállalót foglalkoztató munkáltatóra.

A Társaság a fent megnevezett rendelet alapján köteles továbbítani a vizsgálatban érintett személy (leendő munkavállaló, munkavállaló) adatait, ezt a kötelezettségét a rendelet írja elő: a 15. § (6) bekezdése szerint a Társaság, mint munkáltató a munkaköri alkalmasságot vizsgáló és véleményező szerv kérésére mindazokat a munkaköri és munkahelyi adatokat közli, amelyeket a véleményezéshez szükségesnek tart, illetve amit a véleményező kér. Az egészségügyi szerv a tudomására jutott nem egészségügyi adatokat nem hozhatja nyilvánosságra.

Bár a fent megnevezett rendelet 13. § (5) bekezdése felhatalmazást ad a munkaköri alkalmasság vizsgálatát végző számára, hogy az alkalmatlanság okát a vizsgált személy írásbeli hozzájárulásával közölje munkáltatóval, de a Társaság még a vizsgált személy írásbeli hozzájárulásával sem kezeli semmilyen esetben sem a különleges személyes adatokat.

24.2. A munkaviszony fenntartásával és megszűnésével kapcsolatos adatkezelések

A Társaság munkavállalóiról személyzeti, illetve bér- és munkaügyi nyilvántartást vezet.

A személyzeti nyilvántartás a munkaviszonyra, illetve foglalkoztatásra irányuló egyéb jogviszonyra (pl.: önálló tevékenységként végzett megbízás, vállalkozás stb.) vonatkozó tények dokumentálására szolgáló adatkezelés. A személyzeti nyilvántartás adatai a munkavállaló munkaviszonyával kapcsolatos tények megállapítására és statisztikai adatszolgáltatásra használhatók fel. A személyzeti nyilvántartás a Társaság valamennyi munkavállalójának adatait tartalmazza.

A munkavállalók adatkezelésének jogalapja a törvényi felhatalmazás (munka törvénykönyvéről szóló 2012. évi I. törvény).

24.3. A munkaviszonnal kapcsolatos adatkezelésekre vonatkozó nyilatkozatok

Amennyiben a munkaviszony létesítéséhez, fenntartásához, megszüntetéséhez, az ezekkel kapcsolatos jogosultságok bizonyításához vagy kötelezettségek elismeréséhez nyilatkozat beszerzése szükséges a munkavállalótól, úgy a nyilatkozat beszerzése során a Társaság minden esetben felhívja a munkavállaló figyelmét a nyilatkozaton megadott adatokkal kapcsolatosan az adatkezelés tényére, jogalapjára, céljára.

Amennyiben a nyilatkozat érvényességéhez okmány bemutatása szükséges (személyi igazolvány, diákigazolvány), úgy a Társaság semmilyen módon nem kezeli az okmány fénymásolt vagy szkennelt képét, hanem az arra jogosult munkavállalója aláírásával tanúsítja az okmány bemutatását és annak érvényességét.

24.4. Munkavállalók oktatása

A Társaság fenntartja a jogot, hogy munkavállalók oktatására harmadik féllel szerződjön. Amennyiben az oktatás törvényileg kötött a munkaviszony ellátásához, úgy a harmadik fél a Társaság adatfeldolgozójaként dolgozza fel az adatokat, minden más oktatás esetén a munkavállaló hozzájárulásával kerül a harmadik félhez továbbításra a személyes adat.

24.5. Béren kívüli juttatások

A Társaság fenntartja a jogot, hogy béren kívüli juttatásokat biztosítson a munkavállalók részére és harmadik féllel szerződjön. Amennyiben a munkavállaló a béren kívüli juttatási elemek közül kiválasztja

azon szolgáltatásokat, amelyeket igénybe kíván venni, úgy azon szolgáltatók részére a szolgáltatás igénybevételéhez szükséges adatokat a Társaság továbbítja.

24.6. Szociális támogatási rendszerek

Temetési segély;

Közvetlen hozzátartozó (szülő, gyerek, házastárs/élettárs) halála esetén írásos igény benyújtásával kaphatja a munkavállaló. Egyedi elbírálás, a Társaság saját halottjának tekinti a belső szabályozás vagy ügyvezetői döntés alapján.

Üdülő használat;

Szabad kapacitás függvényében a munkavállalók használhatják, írásos igény benyújtásával.

Lakhatási támogatás:

Meghatározott feltételek teljesülése esetén a Társaság lakhatási támogatást nyújt. Becsatolásra kerül a lakásbérleti szerződés, illetve bizonylat a lakbér befizetéséről.

adatkezelés célja: az igényelt szociális támogatás elbírálása és kifizetése a jogosult részére

kezelt adatok köre: a kérelmet benyújtó neve, e-mail címe, szociális helyzete, amelyre hivatkozik igénylés esetén, esetleg telefonszáma, ha az érintett azt megadja, halotti anyakönyvi kivonat másolata

adatkezelés jogalapja: a GDPR 6. cikk (1) a) szerinti érintetti hozzájárulás

adattárolás határideje: az adatkezelés céljának megvalósulásáig

adatkezelés módja: papíralapon

24.7. Harmadik személyek munkaviszonnal kapcsolatosan megadott adatai

A munkaviszony kapcsán beszerzett harmadik személy adatai (például pótszabadság vagy baleset esetén értesítendő személy megjelölésekor) a szükséges adattartamot meg nem haladóan vehetők fel és kezelhetők.

Abban az esetben, ha a munkavállaló harmadik személy adatait adja meg, úgy a harmadik személytől köteles az adatkezeléshez a harmadik személy hozzájárulást megszerezni, amellyel a Társaság igazolni tudja, hogy a harmadik személy adatainak kezelésére felhatalmazással rendelkezik.

adatkezelés célja: munkaviszony létesítése, teljesítése vagy megszüntetése, az ezekkel kapcsolatos jogosultságok elismerése és kötelezettségek tanúsítása és a munkaviszonnal összefüggő kedvezmények biztosítása

kezelt adatok köre:

munkavállalók kapcsán;

- neve,
- születési neve,
- születési helye és ideje,
- anyja születési neve,
- lakóhelyének címe,
- tartózkodási helye (amennyiben eltérő a lakóhelytől),
- adóazonosító jele,
- társadalombiztosítási azonosító jele (TAJ szám),
- nyugdíjas törzsszám (nyugdíjas munkavállaló esetén),
- nyilatkozat tartozásról,
- nyilatkozat adatbiztonság megtartásáról,
- folyószámla száma,
- munkaviszony kezdő napja,
- biztosítási jogviszony típusa,

- heti munkaórák száma,
 - telefonszáma,
 - végzettséget igazoló okmány másolati példánya,
 - munkaalkalmassági egészségügyi igazolás,
 - munkaköre,
 - orvosi alkalmasság ténye,
 - erkölcsi bizonyítványának
 - o kiállításának dátuma,
 - o okmányszáma,
 - o kérelem azonosítója,
 - a leszámolást követően a munkaköri alkalmassági záró orvosi vizsgálat elvégzésének ténye,
 - a megváltozott munkaképességű munkavállaló megváltozott munkaképességét megalapozó szakértői határozat,
 - főálláson kívüli munkavégzés esetén
 - o jogviszony jellege,
 - o munkáltató neve és székhelye,
 - o a főálláson kívüli munkahelyen teljesített havi átlagos munkaidő,
 - o elvégzendő tevékenység,
 - előző munkaviszonnyal kapcsolatos igazolások:
 - o igazolvány a biztosítási jogviszonyról és az egészségbiztosítási ellátásról
 - o munkáltatói igazolás a jogviszony megszűnéséről
 - o tárgyévi adóalap
 - az Mt. 120. § alapján járó pótszabadság igénybevételével kapcsolatosan
 - o a rehabilitációs szakértői szerv megváltozott munkaképesség megállapítását igazoló okmány fénymásolata,
 - o fogyatékosági támogatásra jogosultságot igazoló okmány fénymásolata,
 - o vakok személyi járadékára jogosultságot igazoló okmány fénymásolata,
- e-mail címe
- pótszabadság, családi adókedvezmény igénybevétele, adómentes természetbeni juttatásnak minősülő kedvezményes utazási igazolvány igénylésének vagy adómentes iskolakezdési támogatás céljából a munkavállaló
- a) 16. életévét be nem töltött hozzátartozójának
- b) 16. életévét betöltött hozzátartozójának, élettársának
- neve, születési neve,
 - születési helye és ideje,
 - lakcíme,
 - anyja neve,
 - társadalombiztosítási azonosító jele (TAJ szám),
 - adóazonosító jele,
 - érvényes diákigazolvány meglétének ténye
- munkaruhát átvevő munkavállalók esetén:
- o lábméret
 - o fej (sapka) méret
 - o testmagasság
 - o póló- és konfekció méret

adatkezelés jogalapja: törvényi felhatalmazás, a munka törvénykönyvéről szóló 2012. évi I. törvény 10. § (1) és (3)) és az 118. § (1) bekezdése, valamint a vonatkozó 2017. évi CL. törvény rendelkezései

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: papíralapon és elektronikusan

A munkavállalói adatok kezelésére vonatkozóan a szabályzata 5. sz. mellékleteként munkavállalói nyilatkozat készült, amelyeknek célja a munkavállalók előzetes tájékoztatása az adatkezelésről.

24.8. Munkavégzésre irányuló egyéb jogviszonyban foglalkoztatott személyek adatkezelése

A Társaság a munkavállalókon kívül egyes feladatok ellátására munkavégzésre irányuló egyéb jogviszonyban is foglalkoztat szerződéses partnereket a Ptk. szabályai szerint. E személyek adatkezelésével kapcsolatos szabályok az alábbiak:

adatkezelés célja: munkavégzésre irányuló egyéb jogviszony létesítése, teljesítése vagy megszüntetése, az ezekkel kapcsolatos jogosultságok elismerése és kötelezettségek tanúsítása

kezelt adatok köre: név, cím, adószám, anyja neve, valamint a személyes kapcsolattartó neve és telefonszáma, erkölcsi bizonyítványa kiállítási dátuma, okmányszáma, kérelem azonosítója

adatkezelés jogalapja: GDPR 6 cikk. (1) b) szerinti szerződéses kötelezettség teljesítése

adattárolás határideje: az adatkezelés céljának megvalósulásáig, főszabály szerint

- a munkavégzésre irányuló egyéb jogviszonnyal kapcsolatos jogosultságokkal és kötelezettségekkel kapcsolatosan a jogviszony megszűnéséig
- munkavégzésre irányuló egyéb jogviszonyból fakadó jogosultságokkal kapcsolatosan a nyugdíjfolyósításról szóló jogszabályokban meghatározott határideig

adatkezelés módja: papíralapon és elektronikusan

24.9. Diák munkavállalók adatkezelése

A diák munkavállalókat a különböző diákszövetkezetek foglalkoztatják. A diákok személyes adatainak kezelését illetően az Mt. előírásait kell alkalmazni.

A diákok esetében a munkavállalással összefüggésben az alábbi adatokat kezelheti a Társaság:

adatkezelés célja: a diákokra foglalkoztatására vonatkozó jogviszony (jellemzően a diákszövetkezettel kötött szerződés) létesítése, teljesítése, a teljesítés igazolása vagy megszüntetése, az ezekkel kapcsolatos jogosultságok elismerése és kötelezettségek tanúsítása, az érintettekkel való kapcsolattartás

kezelt adatok köre:

- név,
- születési idő,
- értesítési cím,
- telefonszám,
- e-mail cím,

adatkezelés jogalapja: törvényi felhatalmazás, a munka törvénykönyvéről szóló 2012. évi I. törvény 10. § (1) és (3)]

adattárolás határideje: az adatkezelés céljának megvalósulásáig, főszabály szerint

- diákok foglalkoztatására vonatkozó jogviszonnyal kapcsolatos jogosultságokkal és kötelezettségekkel kapcsolatosan a munkaviszony megszűnéséig

adatkezelés módja: papíralapon és elektronikusan

25. A munkavállalók ellenőrzésével kapcsolatos adatkezelés

A munkáltató a munkaviszonnyal összefüggő magatartása körében ellenőrizheti a munkavállalókat. Az ellenőrzésre az Mt. 11. § (1)-(2) bekezdése ad jogalapot.

A Társaság az Mt.-ben meghatározott jogalappal ellenőrzi munkavállalóit. A Társaság előzetesen tájékoztatja a munkavállalót azoknak a technikai eszközöknek az alkalmazásáról, amelyek a munkavállaló ellenőrzésére szolgálnak.

25.1. Céges eszközök ellenőrzése

A Társaság a munkavállalóknak indokolt esetben, munkavégzés céljára biztosít számítógépet, e-mail címet és internet-hozzáférést. A használat szabályairól és az ellenőrzés lehetőségéről a munkavállalókat a Társaság előzetesen írásban tájékoztatja.

Mivel a Társaság tulajdonát képező személyi számítógépeket és laptopokat, céges e-mail címeket a Társaság munkavégzés céljából biztosítja, azokon személyes adatot tárolni tilos. Amennyiben a munkavállaló a tiltás ellenére 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. Erről (illetve az archiválás és a rendszergazdai tevékenység tényéről) a munkavállalókat az eszközök használata előtt írásban tájékoztatja a Társaság.

25.2. Céges e-mail címek ellenőrzése

A Társaság munkavállalói tudomásul veszik, hogy mindazon e-mail címek, amelyekben a Társaság neve kiterjesztésként szerepel (...@kemenysepro.hu), a Társaság tulajdonát képezik és az ezen a címen folytatott levelezés munkacélú levelezésnek minősül. A fogadott és küldött e-mailek tartalma a Társaság tulajdonát képezik.

Az ilyen címen folytatott levelezésbe a Társaság megfelelő jogalap esetén jogosult betekinteni. A Társaság jogosult a fent nevezett címen folytatott levelezések meghatározott időközönkénti biztonsági mentésére, az elektronikus levelező rendszer folyamatosságának és stabilitásának érdekében.

A céges e-mail címen nem munkavégzési célú (magán vagy bármilyen egyéb) levelezést tilos folytatni. Amennyiben a munkavállaló a céges e-mail címén „(...@kemenysepro.hu)” található leveleiben magán- vagy bármilyen egyéb célú levelezést folytat, ezzel egy időben a postafiókban magáncélú személyes adatait tárolja, úgy a Társaság az e-mail cím ellenőrzése során ezeket az adatokat is megismerheti.

Mindemellett főszabály szerint a magáncélú levelek tartalmát a munkáltató munkaviszonyból fakadó jogosultság érvényesítése során sem jogosult megismerni, továbbá amíg a munkaviszonnyal kapcsolatos jog vagy kötelezettség teljesítéséhez nincs rá szükség, addig nem is célja magánjellegű adatok megismerése.

25.3. Céges telefonhasználat

A céges mobiltelefonok használata során a személyi jövedelemadóról szóló 1995. évi CXVII. törvény 70. §-ának (5) bekezdés ca) pontjában foglaltak alapján ellenőrizhet a Társaság. A Társaság minden céges mobiltelefonnal rendelkező munkavállalóval egyedi megállapodást köt a céges mobilhasználat részletszabályainak rögzítése céljából. A munkavállaló a megállapodás aláírásával kifejezetten hozzájárul ahhoz, hogy a keretösszeg felhasználásának ellenőrzése céljából a Munkáltató betekintsen a hívott fél adatait nem tartalmazó hívásrészletezőbe.

25.4. Az ellenőrzés menete

A Társaság a tulajdonában álló minden eszközt ellenőrizhet a fokozatosság elvének betartásával, valamint a munkavállaló jelenlétének biztosításával.

Az ellenőrzés tényéről az ellenőrzés céljával összefüggően tájékoztatja az ellenőrzéssel érintett munkavállalót. A technikai ellenőrzést a rendszergazda végezheti alkalmi vizsgálatok lefolytatásával, de akár a Társaság bármely munkavállalója által kérelmezhető, amennyiben a Társaság gazdasági érdekeit veszélyeztető folyamat valószínűsíthető.

adatkezelés célja: a Társaság jogos üzleti érdekeinek megfelelően a munkavállalók Mt. 11. § (1) 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, a munkajogviszony ellátása során észlelt jogsértés ténye, a jogsértés leírása

adatkezelés jogalapja: 2012. évi I. törvény 11. § (1)

adattárolás határideje: az ellenőrzéstől számított 1 év, de legkésőbb az ellenőrzéssel kapcsolatos igény elévülése

adatkezelés módja: elektronikusan

25.5. GPS alkalmazása

A Társaság gépjárműveiben GPS található, amelynek segítségével a gépjármű mozgása nyomon követhető. Az eszköz rögzíti a futásteljesítményt, az útvonalat, a megállóhelyeket és a tartózkodás idejét, stb. Az adatokhoz hozzá van rendelve a rendszám, a vezető neve, sofőr kódja és a dátum.

A GPS adatokat (és az ehhez kapcsolódó személyes adatokat) a fenti módon a külső szolgáltató látja, adatfeldolgozóként.

A Társaság egyes munkavállalók számára engedélyezi a céges gépjárművek magánhasználatát a túlfutás és az üzemanyagköltség megtérítése ellenében. Magánhasználat esetén a GPS adatok korlátozottan hozzáférhetők munkáltató részére. A magánhasználat kapcsán kezelt adatok köre: időszak és futott kilométer (távolság).

adatkezelés célja: az céges gépjárművek használata során a gépjármű útvonalának, megállóhelyeinek nyomon követése, a Társaság jogos üzleti érdekének érvényesítése, valamint a rendkívüli események (lopás, baleset) észlelése céljából

kezelt adatok köre: munkavállaló neve, GPS koordináták, megtett útvonal és megállóhelyek, riasztás esetén a riasztás és a rendkívüli esemény tényének jelzése

adatkezelés jogalapja: az Mt. 10. § (1) és a 11. § (1) bekezdése

adattárolás határideje: az adatkezelési cél megvalósulásáig, az ellenőrzéssel kapcsolatos igény elévüléséig, maximálisan az adatfelvételtől számított 5 évig

adattárolás módja: papíralapon és elektronikusan

26. Céges biztosítással kapcsolatos adatkezelés

A munkavállalók az alábbiakat vehetik igénybe:

- csoportos élet és balesetbiztosítás.

A vezető tisztségviselők és a felügyelőbizottsági tagok az alábbi:

- felelősségbiztosítás.

Adatkezelés valósul meg továbbá: CASCO és KGFB biztosításokkal összefüggésben baleset esetén (baleseti bejelentőn rögzített személyes adatok)

A biztosítások kapcsán az alábbi adatok kerülnek továbbításra:

- személyi igazolványon, lakcím kártyán, vezetői engedélyen, amennyiben gépjárművel kapcsolatos a károkozás, amennyiben a vagyonban történik a károkozás, abban az esetben az eltűnt tárgy korábbi számláját vagy annak másolatát, a beszerzési értékét küldik meg a személyes adatok mellett a biztosítónak.

A küldött dokumentumokat a kárigény bejelentővel együtt lefűzésre kerülnek, zárt lemezszekrényben.

adatkezelés célja: kárigény esetén a kárigény benyújtása a biztosító társaság felé

kezelt adatok köre:

- dolgozói név, születési hely, idő, lakcím, anyja neve, TAJ szám, valamint az elhunyt halotti anyakönyvi kivonat, születési anyakönyvi kivonat, halotti vizsgálati bizonyítvány és zárójelentés,
- orvosi dokumentáció másolata (zárójelentés, kórházi igazolás, ambuláns kezelőlap stb.)
- károkozás esetén a fent felsorolt elemek

adatkezelés jogalapja: a GDPR 6. cikk (1) a) szerinti érintetti hozzájárulás, valamint a GDPR 9. cikk (2) f)

adattárolás határideje: az adatkezelés céljának megvalósulásáig

adatkezelés módja: papíralapon és elektronikusan

Ezen adatkezelésről tájékoztató készült, amely jelen szabályzat 6. sz. melléklete.

27. Elektronikus megfigyelőrendszer alkalmazása

A Társaság elektronikus megfigyelőrendszert üzemeltet az alábbi helyeken:

- székhely és ügyfélszolgálat: 1145 Budapest, Szugló utca 9-15.
- parkoló: 1145 Budapest, Columbus utca 7.
- parkoló, főbejárat, ügyfélszolgálat és 1. emeleti folyosó: 1032 Budapest, Kiscelli út 65.
- parkol és 3. emelet: 1191 Budapest, Üllői út 206.

27.1. Kamerafigyeléssel összefüggő adatkezelés

A Társaság a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól szóló 2005. évi CXXXIII. törvényben (a továbbiakban: Szvtv.) meghatározottak szerint elektronikus megfigyelőrendszert üzemeltet.

A Társaság fenntartja magának a jogot, hogy az elektronikus megfigyelőrendszert különböző célok szerint üzemeltesse.

A Társaság az elektronikus megfigyelőrendszerrel megfigyelt területeket három különálló kategóriába sorolja a megfigyelés célja alapján, mely különálló kategóriáknak az Szvtv. különböző megőrzési időt tesz lehetővé.

Az I. kategóriába sorolható az emberi élet, testi épség védelmére irányuló megfigyelési cél. Az első kategóriába tartozó kameraképek tárolási idejére az Szvtv. 31. § (1)- (2) bekezdései szerinti főszabály, a három munkanapos tárolási határidő érvényesül.

A II. kategóriában megfigyelési célként a Büntető Törvénykönyvről szóló törvény szerint legalább jelentős értékű vagyontárgy védelme és biztonságos tárolása és az emberi élet, testi épség védelme teljesül. Ebben a kategóriában az Szvtv. 31. § (3) bekezdés c) pontja szerint harminc napos tárolási határidő érvényesül.

A III. kategóriába tartozik a pénzügyi szolgáltatást és kiegészítő pénzügyi szolgáltatást folytatóknak a feladat ellátásaihoz szükséges, a közönség számára nyilvános magánterületének védelme érdekében történő rögzítés, az Szvtv. 31. § (4) bekezdés a) pontja értelmében, mely szerint hatvan napos tárolási idő érvényesíthető.

Az elektronikus megfigyelőrendszer által készített képek megőrzésére és felhasználására az Szvtv. rendelkezéseinek figyelembe vételével az alábbi szabályok irányadóak:

27.2. Az elektronikus megfigyelőrendszerrel készített felvételek törlésének módja és határideje

I. szektor

A felvétel felhasználás hiányában a rögzítéstől számított 3, azaz három munkanap elteltével törlésre kerül [Szvtv. 31. § (2)]. Felhasználásnak az minősül, ha a felvételt bírósági vagy más hatósági eljárásban bizonyítékként felhasználják.

II. szektor

A felvétel felhasználás hiányában a rögzítéstől számított 30, azaz harminc nap elteltével törlésre kerül [Szvtv. 31. § (3) c)]. Felhasználásnak az minősül, ha a felvételt bírósági vagy más hatósági eljárásban bizonyítékként felhasználják.

III. szektor

A felvétel felhasználás hiányában a rögzítéstől számított 30, azaz harminc nap elteltével törlésre kerül [Szvtv. 31. § (3) d)]. Felhasználásnak az minősül, ha a felvételt bírósági vagy más hatósági eljárásban bizonyítékként felhasználják.

Közös szabályok

Minden szektor esetében biztosítja a Társaság az érintetti jogok közül az Szvtv-ben meghatározottat, tehát az, akinek jogát vagy jogos érdekét a felvétel rögzítése érinti, a felvétel fent meghatározott törlési idején (három munkanapon vagy harminc napon) belül jogának, vagy jogos érdekének igazolásával kérheti, hogy az adatot annak kezelője ne semmisítse meg, illetve ne törölje. A kérelemről a lehető legrövidebb időn belül az adatvédelmi tisztviselő dönt. Az így megjelölt felvételt ki kell menteni és átadni az adatvédelmi tisztviselőnek, aki gondoskodik annak jelen Szabályzat szerinti megfelelő őrzéséről. Bíróság vagy más hatóság megkeresésére a rögzített felvételt a bíróságnak vagy a hatóságnak haladéktalanul meg kell küldeni. Amennyiben megkeresésre attól számított harminc napon belül, hogy a megsemmisítés mellőzését kérték, nem kerül sor, a felvétel törlésre kerül.

27.3. Az elektronikus megfigyeléssel kapcsolatos garanciális szabályok

A Társaság az elektronikus megfigyelőrendszerrel csak a szükséges mértékben avatkozik bele az érintettek magánszférájába.

A Társaság semmilyen indokból és módon nem folytat elektronikus megfigyelést:

- abból a célból, hogy egy munkavállaló munkaintenzitását megfigyelje,
- abból a célból, hogy a munkavállalók munkahelyi viselkedését a befolyásolja,
- szenzitív területeken, így különösen öltözőben, zuhanyzóban, illemhelyiségben,
- olyan területen, ahol a munkavállalók pihenőidejüket vagy munkaközi szünetüket töltik, különösen pihenőszobában, dohányzásra kijelölt helyen.
- közterületen.

A Társaság azonban abból a célból folytathat elektronikus megfigyelést, hogy meggyőződjön róla, hogy az egészséget nem veszélyeztető és biztonságos munkavégzés érdekében a munkavállalók megtartják-e a rájuk vonatkozó rendelkezéseket.

27.4. Az érintettek tájékoztatása

Az adatkezelésre vonatkozóan tájékoztató készült, amelynek célja az érintettek előzetes tájékoztatása az adatkezelésről. A tájékoztató a szabályzat 9., 10 és 11. számú melléklete. A tájékoztatók a megfigyelt területre történő összes belépési ponton és az I, II és a III. szektor közötti átjárási pontokon kerülnek kihelyezésre.

27.5. A Társaság munkavállalóinak tájékoztatása

Az adatkezelésre vonatkozóan munkavállalói tájékoztatók készültek, amelyeknek célja a munkavállalók előzetes tájékoztatása az adatkezelésről. A tájékoztató szövegét a szabályzat 9., 10 és 11. számú

mellékletei tartalmazzák, valamint külön utasítás került kibocsátásra e témakörben a Társaság vezető tisztségviselője által.

27.6. A kameraképek megtekintése

Annak érdekében, hogy Társaság minél kevésbé terjeszkedjen bele az érintettek magánszférájába, az elektronikus megfigyelőrendszerrel készített felvételekhez csak meghatározott személyek férhetnek hozzá.

A Társaság szervezetrendszerén belül a jelen Szabályzatban is kijelölt személy jogosult a felvételeket megtekinteni.

Élőképet a székhelyen látnak. A rögzített felvételekhez a Társaság kijelölt vezetői férnek hozzá.

A Társaság által megvalósított elektronikus megfigyelés során csak a szabályzat 12. sz. mellékletében felsorolt személyek rendelkeznek betekintési joggal. Az adatokat a visszavonástól számított max. 5 éven keresztül őrzi meg a Társaság.

A kamerás képekbe történő betekintésről a szabályzat 13. sz. melléklete szerinti jegyzőkönyvet kell készíteni.

27.7. A kameraképek zárolása

Kamerakép zárolását csak a Társaság kamerarendszere által megvalósított adatkezelés felügyeletére kijelölt személy vagy az adatvédelmi tisztviselő rendelheti el.

Kamerakép zárolását kezdeményezheti

- a Társaságnál betekintési joggal rendelkező személy, amennyiben a felvételekbe való betekintés során olyan körülményt észlel, amely veszélyezteti az elektronikus megfigyelőrendszerrel elérni kívánt célt,
- bárki, akinek jogát vagy jogos érdekét a felvétel érinti.

Felvétel zárolását csak a kamerarendszer által megvalósított adatkezelés felügyeletére kijelölt személynek és ezzel egyidőben az adatvédelmi tisztviselőnek címzett írásbeli kérelemmel lehet kérvényezni.

A zárolásról a lehető legrövidebb időn belül a Társaság kamerarendszer által megvalósított adatkezelés felügyeletére kijelölt személye (az adatvédelmi tisztviselővel egyetértésben) dönt.

A Társaság minden, a kamerával rögzített képekből történő zárolásról jegyzőkönyvet vesz fel, amiben rögzíteni kell a betekintés és a zárolás időpontját, célját és a zárolásra okot adó eseményt és a további felhasználás megjelölését. Az erről szóló jegyzőkönyv a szabályzat 18. sz. melléklete.

27.8. Zárolási jogosultsággal rendelkező személyek

A Társaság a zárolásra jogosultak köréről is nyilvántartást vezet. A nyilvántartás része a zárolási joggal rendelkező személy neve és munkaköre, a zárolási jog kiadásának dátuma, a zárolási jog visszavonásának dátuma. Az adatokat a visszavonástól számított 5 éven keresztül őrzi meg a Társaság. A zárolási jogosultsággal rendelkező személyek nyilvántartása a szabályzat 15. sz. melléklete.

27.9. I. szektor

adatkezelés célja: az objektum biztonságának és a Társaság vagyoni javainak megóvása, valamint a megfigyelt területen tartózkodó személyek testi épségének és vagyoni javainak megóvása vagyoni védelmi célból

kezelt adatok köre: az érintett képmása, a kameraképpel megszerezhető adatok (tartózkodási hely, tartózkodási idő)

adatkezelés jogalapja:

- külső személyek vonatkozásában: az érintett ráutaló magatartással tanúsított hozzájárulása [Szvtv. 30. § (2)]
- munkavállalók vonatkozásában: GDPR 6. cikk (1) f) szerinti érdekmérlegelés alapján

adattárolás határideje:

- a felvétel felhasználás hiányában a rögzítéstől számított 3, azaz három munkanap elteltével törlésre kerül [Szvtv. 31. § (2)],
- amennyiben a felvételt jog vagy jogos érdek igazolásával kérték, hogy a Társaság azt ne semmisítse meg, ám a megkeresésre nem kerül sor, úgy a megkereséstől számított 30, azaz harminc nap elteltével törlésre kerül [Szvtv. 31. § (6)]

adatkezelés módja: elektronikusan

27.10. II. szektor

adatkezelés célja: a Büntető Törvénykönyvről szóló törvény szerint legalább jelentős értékű vagyontárgy biztonságos tárolása, kezelése, szállítása

kezelt adatok köre: az érintett képmása, a kameraképpel megszerezhető adatok (tartózkodási hely, tartózkodási idő),

adatkezelés jogalapja:

- külső személyek vonatkozásában: az érintett ráutaló magatartással tanúsított hozzájárulása [Szvtv. 30. § (2)]
- munkavállalók vonatkozásában: GDPR 6. cikk (1) f) szerinti érdekmérlegelés alapján

adattárolás határideje:

- a felvétel felhasználás hiányában a rögzítéstől számított 30, azaz harminc nap elteltével törlésre kerül [az Szvtv. 31. § (3) c)]
- amennyiben a felvételt jog vagy jogos érdek igazolásával kérték, hogy a Társaság azt ne semmisítse meg, ám a megkeresésre nem kerül sor, úgy a megkereséstől számított 30, azaz harminc nap elteltével törlésre kerül [Szvtv. 31. § (6)]

adatkezelés módja: elektronikusan

27.11. III. szektor

adatkezelés célja: veszélyes anyagok őrzése

kezelt adatok köre: az érintett képmása, a kameraképpel megszerezhető adatok (tartózkodási hely, tartózkodási idő),

adatkezelés jogalapja:

- külső személyek vonatkozásában: az érintett ráutaló magatartással tanúsított hozzájárulása [Szvtv. 30. § (2)]
- munkavállalók vonatkozásában: GDPR 6. cikk (1) f) szerinti érdekmérlegelés alapján

adattárolás határideje:

- a felvétel felhasználás hiányában a rögzítéstől számított 30, azaz harminc nap elteltével törlésre kerül [az Szvtv. 31. § (3) d)]
- amennyiben a felvételt jog vagy jogos érdek igazolásával kérték, hogy a Társaság azt ne semmisítse meg, ám a megkeresésre nem kerül sor, úgy a megkereséstől számított 30, azaz harminc nap elteltével törlésre kerül [Szvtv. 31. § (6)]

adatkezelés módja: elektronikusan

Jelen szabályzat kiadásakor a III. szektorba tartozó adatkezelést nem valósít meg a Társaság.

28. Beléptetéssel összefüggő adatkezelés

A Társaság sem elektronikus, sem papír alapú beléptető rendszert nem alkalmaz a székhelyen található Ügyfélszolgálaton, az Ügyfélszolgálati iroda ügyfélfogadási időben bárki számára látogatható és nyitva áll.

Ettől eltérő a munkavégzésre szolgáló egyéb irodák beléptetése, amelyek azonban nem azonos szinten helyezkednek el az Ügyfélszolgálati irodával, így oda csak az arra jogosult személyek léphetnek be.

A Társaság székhelyén portaszolgálatot üzemeltet az irodaház tulajdonosa, így ezen adatkezelésnek az adatkezelője minden esetben az irodaház tulajdonosa.

A Társaság semmilyen beléptetési adatot nem kezel, valamint azok a részére nincsenek továbbítva.

29. Munkára képes állapot ellenőrzése

Az alkoholfogyasztásra a Társaságnál zéró tolerancia van érvényben.

Az ellenőrzésre bármely munkakörben sor kerülhet. Az alkoholfogyasztás megalapozhatja az azonnali hatályú felmondást.

Az Mt. 52. § (1) a) kimondja, hogy a munkavállaló és a munkavégzésre irányuló egyéb jogviszonyban foglalkoztatott személy köteles a munkáltató által előírt helyen és időben munkára képes állapotban megjelenni.

Az Mvt. 2. § (3)-ban kapott felhatalmazás alapján az alábbiak szerint határozza meg az alkoholos befolyásoltságra vonatkozóan az egészséget nem veszélyeztető és biztonságos munkavégzés követelményeinek megvalósítását:

Az Mvt. 60. § (1) alapján a munkavállaló és a munkavégzésre irányuló egyéb jogviszonyban foglalkoztatott személy csak a biztonságos munkavégzésre alkalmas állapotban, a munkavédelemre vonatkozó szabályok, utasítások megtartásával, a munkavédelmi oktatásnak megfelelően végezhet munkát. A munkavállaló köteles munkatársaival együttműködni és munkáját úgy végezni, hogy ez saját vagy más egészségét és testi épségét ne veszélyeztesse.

A Társaság minden feladatkörre vonatkozóan tiltja, hogy a munkavállalói alkoholos befolyásoltság alatt tartózkodjanak a munkavégzés területén – ez vonatkozik arra az esetre is, ha a érintett munkaidején túl, már/még nem munkavégzési céllal tartózkodik a területen, lévén az alkoholos befolyásoltság alatt álló személy veszélyezteti mások biztonságos munkavégzését. Tilos a Társaság területére vagy amennyiben az nem azonos vele, úgy a munkavégzés területére alkoholos befolyásoltság alatt belépni, ott alkoholt fogyasztani, alkoholos befolyásoltság alatt munkát végezni.

A Társaság a biztonságos munkavégzés követelményeit kialakítandó kötelezettségénél fogva köteles rendszeresen meggyőződni arról, hogy a munkavállalók megtartják-e a rájuk vonatkozó rendelkezéseket. A munkajogi előírások betartásának ellenőrzésére vonatkozó szabályokat mind az Mt., mind az Mvt. pontosítja.

Mt. 11. § (1) A munkáltató a munkavállalót csak a munkaviszonnyal összefüggő magatartása körében ellenőrizheti. A munkáltató ellenőrzése és az annak során alkalmazott eszközök, módszerek nem járhatnak az emberi méltóság megsértésével. A munkavállaló magánélete nem ellenőrizhető.

Mvt. 54. § (7) b) Az egészséget nem veszélyeztető és biztonságos munkavégzés érdekében a munkáltató köteles rendszeresen meggyőződni arról, hogy a munkakörülmények megfelelnek-e a követelményeknek, a munkavállalók ismerik, illetve megtartják-e a rájuk vonatkozó rendelkezéseket.

A munkára alkalmasság ellenőrzéséről a Társaság saját, belső Munkavédelmi Szabályzata rendelkezik az alábbiak szerint:

5.1.10. A munkahelyen munkaidő alatt szeszes italt fogyasztani tilos! Alkoholos vagy más, egészségre ártalmas szer hatása alatt álló dolgozót a munkahelyre beengedni, foglalkoztatni, jogszabály szerint nem szabad.

Az alkoholszondás vizsgálatnak valamennyi dolgozó köteles magát alávetni. Amennyiben ezt megtagadja, alkohol által befolyásoltnak kell tekinteni.

A Kft. minden dolgozójánál alkoholszondás vizsgálatot végezhetnek az alábbi vezetők:

- a) Ügyvezető,
- b) Műszaki igazgató,
- c) Gazdasági igazgató,
- d) Osztályvezetők (saját munkaterületen),
- e) Régióvezetők (saját munkaterületen),
- f) Biztonsági irodavezető,

Az alkoholszondás vizsgálat eredményét jegyzőkönyvben, két tanú jelenlétében dokumentálja a Társaság.

adatkezelés célja: munkára alkalmas állapot ellenőrzése munkavédelmi célból

kezelt adatok köre: az ellenőrzés eredménye, időpontja, munkára alkalmas állapot ténye, ellenőrzést végző személy adatai, ellenőrzés alá vont munkavállaló adatai. Ha az ellenőrzött személy vitatja az eredményt, akkor annak ténye is, illetve pozitív minta esetén, ha lemond a vérvizsgálat jogáról, akkor ennek a ténye is.

adatkezelés jogalapja: a munkavédelemről szóló 1993. évi XCIII. törvény 60. § (1), valamint a munka törvénykönyvéről szóló 2012. évi I. törvény 11. § (1) és (2) bekezdés

adattárolás határideje: az ellenőrzésből fakadó jogok és kötelezettségek által megalapozott igények érvényesítésére nyitva álló határidő

adattárolás módja: papíralapon és elektronikus