

**Enyingi Agrár Zártkörűen működő Részvénytársaság**  
8134 Mátyásdomb-Ágostonpuszta

**ADATVÉDELMI ÉS KEZELÉSI SZABÁLYZAT**

**2022. február 15.**

# I.

## Általános rendelkezések

### 1. A szabályzat célja:

Az adatvédelmi - adatkezelési szabályzat célja, hogy az Enyingi Agrár Zrt (székhely: 8134 Mátyásdomb, Ágostonpuszta 0174/32 hrsz ; elektronikus levelezési cím: agoston@eagrt.hu , adószám: 11106131-2-07 ) adatok kezelésével, felhasználásával, védelmével, továbbításával, kapcsolatos szabályait, előírásait rögzítse.

Az Adatvédelmi és Kezelési Szabályzat célja, hogy meghatározza az Enyingi Agrár Zrt.-nél, mint Adatkezelőnél zajló adatkezelések törvényes kereteit, biztosítsa az adatvédelem alkotmányos elveinek és az információs önrendelkezési jognak az érvényesítését, elősegítse az adatbiztonság követelményeinek való megfelelést, továbbá megakadályozza a jogosulatlan adatkezelést.

Az Adatvédelmi és Kezelési Szabályzat kialakítja az adatvédelem szempontjából fontos feladatokat, felelősségi viszonyokat, különös tekintettel a munkavállalók szerepére az adatbiztonságban.

A szabályzat célja továbbá, hogy az informatikai rendszer alkalmazása során biztosítsa az adatvédelem elveinek, az adatbiztonság követelményeinek érvényesülését, s megakadályozza a jogosulatlan hozzáférést, az adatok megváltoztatását és jogosulatlan nyilvánosságra hozatalát.

A szabályzat további céljai:

- a titok, vagyon- és tűzvédelemre vonatkozó védelmi intézkedések meghatározása, betartása
- az üzemeltetett informatikai rendszerek rendeltetésszerű használata
- az üzembiztonságot szolgáló karbantartás és fenntartás
- az adatok informatikai feldolgozása és azok további hasznosítása során az illetéktelen felhasználásból származó hátrányos következmények megszüntetése, illetve minimális mértékre való csökkentése
- adatállományok tartalmi és formai épségének megőrzése
- az alkalmazott programok és adatállományok dokumentációinak nyilvántartása
- a munkaállomásokon lekérdezhető adatok körének meghatározása
- az adatállományok biztonságos mentése
- az informatikai rendszerek zavartalan üzemeltetése
- a feldolgozás folyamatát fenyegető veszélyek megelőzése, elhárítása
- az adatvédelmi és adatbiztonság feltételeinek megteremtése.

### 2. A szabályzat hatálya:

Jelen Szabályzat hatálya kiterjed az Enyingi Agrár Zrt. által végzett valamennyi adatkezelésre, adattovábbításra, információ átadásra, az ezen adatkezelés, információátadás tárgyát képező

adat, jelen Szabályzatban meghatározottak szerinti, üzleti titokként kezelésével és védelmével kapcsolatos tevékenységekre.

Jelen Szabályzat hatálya kiterjed az Enyingi Agrár Zrt. egyes szervezeti egységei közötti adatáramlásra, valamint az Enyingi Agrár Zrt más adatkezelőkkel való személyes adatokat érintő kommunikációjára.

A Szabályzat személyi hatálya kiterjed az Enyingi Agrár Zrt. valamennyi szervezeti egységére, minden alkalmazottjára, valamint az adatok alapján érintett személyekre.

A Szabályzat tárgyi hatálya kiterjed az Enyingi Agrár Zrt. szervezeti egységei által kezelt valamennyi személyes és egyéb adatra, a rajtuk végzett adatkezelési műveletek teljes körére, keletkezésük, kezelésük, feldolgozásuk helyétől, valamint megjelenési formájuktól függetlenül.

A szabályzat a fentiek alapján kiterjed

- a társaság által kezelt személyes adatok körére, felhasználási területére, ezek keretében a cél és a tárolhatóság elveinek rögzítésére,
- a társaság által kezelt egyéb adatok körére, felhasználási területére, ezek keretében a cél és a tárolhatóság elveinek rögzítésére,
- a teljes informatikai rendszerre, továbbá
- a védelmet élvező elektronikus adatok teljes körére, felmerülésük és feldolgozási helyüktől, idejüktől és az adatok fizikai megjelenési formáitól függetlenül
- a társaság tulajdonában lévő, illetve általa használt valamennyi informatikai berendezésre
- az informatikai eszközök műszaki dokumentációjára
- az informatikai folyamatban szereplő összes dokumentációra
- a rendszer és felhasználói programokra
- az adatok felhasználására
- az adathordozók tárolására, felhasználására
- a társaság által üzemeltetett kamerákra, az azok által rögzített felvételekre

Az adatvédelmi szempontokat már a folyamatok, rendszerek tervezésénél követelményként kell kezelni és be kell építeni az üzleti és informatikai szakértők munkájába, az adatkezelés módjának meghatározásakor.

### **3. A védelmet igénylő adatok és információk minősítése, hozzáférési jogosultság**

A személyes adatokat, és az egyéb adatokat és információkat jelentőségük szerint az alábbiak szerint osztályozzuk

- bárki által megismerhető
- korlátozottan megismerhető
- minősített, titkos

Az adatok minősítését a vezérigazgató végzi el.

Az adatok feldolgozásakor meg kell határozni írásban és névre szólóan a hozzáférési jogosultságot.

Alapelv, hogy mindenki csak ahhoz az adathoz jusson hozzá, amire a munkájához szüksége van.

Jelen Szabályzatot a társaság vezérigazgatója hagyja jóvá. A Szabályzatot legalább évente felül kell vizsgálni.

A Szabályzat valamennyi munkavállaló számára papír alapon a titkárságon elérhető.

A Szabályzat végrehajtásáért saját szervezetükön belül a felsővezetők felelősek. Valamennyi munkavállaló kötelezettsége annak bejelentése, ha a Szabályzat megkerüléséről vagy megsértéséről szerez tudomást, vagy ennek gyanúja merül fel.

#### **4. Jogszabályi alapok, kapcsolat a társaság egyéb szabályzataival**

Jelen Adatvédelmi és kezelési Szabályzat jogszabályi alapját a következő törvények jelentik:

- Magyarország Alaptörvénye;
- 2011. évi CXII. törvény - az információs önrendelkezési jogról és az információszabadságról (a továbbiakban: Infotv.);
- 2012. évi I. törvény – a munka törvénykönyvéről
- 2013. évi V. törvény – a Polgári Törvénykönyvről
- EU rendelet
- 2019.évi XXXIV tv
- **2021. évi CXXII törvény**

Jelen Adatvédelmi és kezelési Szabályzat az alábbi belső szabályzatokhoz kapcsolódik, azokkal együttesen értelmezendő:

- Bérszabályzat;
- Érdekeltségi rendszer
- Képviseleti és utalványozási szabályzat
- Pénzügyi szabályzat
- Rendészeti szabályzat

#### **5. Az adatkezelésre vonatkozó fontosabb információk**

**Adatkezelő neve:** Enyingi Agrár Zártkörűen működő Részvénytársaság ( cégjegyzékszám: 07-10-001081)

**Adatkezelő elérhetősége:**

székhely: 8134 Mátyásdomb, Ágostonpuszta 0174/32 hrsz

telefonszám: 22- 372-014, 22/ 436-454, 30-5609-401,30-5609-402, 30-5609-426

fax: 22-436-461

email: [agoston@eagrt.hu](mailto:agoston@eagrt.hu)

**Adatkezelő képviselőjének neve:** Szávay Gábor vezérigazgató

## **Adatkezelő képviselőjének elérhetősége:**

8134 Mátyásdomb, Ágostonpuszta 0174/32 hrsz

telefonszám: 22- 372-014,22-436-454,30-5609-401, 30-5609-402

email: agoston@eagrt.hu

## **II.**

### **A társaság által kezelt személyes adatok és azok védelme**

#### **1. A személyes adatok védelmével kapcsolatos fogalmak:**

**érintett:** bármely információ alapján azonosított vagy azonosítható természetes személy;

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

**személyes adat:** az érintetthez vonatkozó bármely információ;

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

**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 adott természetes személyből vett biológiai minta elemzéséből ered;

**biometrikus adat:** egy természetes személy fizikai, fiziológiai vagy viselkedési jellemzőire vonatkozó olyan, sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását, mint például az arckép vagy a daktiloszkópiai adat;

**egészségügyi adat:** egy természetes személy testi vagy szellemi 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;

**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;

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

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

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

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

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

**bűnüldözési célú adatkezelés:** a jogszabályban meghatározott feladat- és hatáskörében a közrendet vagy a közbiztonságot fenyegető veszélyek megelőzésére vagy elhárítására, a bűnmegelőzésre, a bűnfelderítésre, a büntetőeljárás lefolytatására vagy ezen eljárásban való közreműködésre, a szabálysértések megelőzésére és felderítésére, valamint a szabálysértési eljárás lefolytatására vagy ezen eljárásban való közreműködésre, továbbá a büntetőeljárásban vagy szabálysértési eljárásban megállapított jogkövetkezmények végrehajtására irányuló tevékenységet folytató szerv vagy személy (a továbbiakban együtt: bűnüldözési adatkezelést folytató szerv) ezen tevékenység keretei között és céljából - ideértve az ezen tevékenységhez kapcsolódó személyes adatok levéltári, tudományos, statisztikai vagy történelmi célból történő kezelését is - (a továbbiakban együtt: bűnüldözési cél) végzett adatkezelése;

**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;

**adatkezelés korlátozása:** a tárolt adat zárolása az adat további kezelésének korlátozása céljából történő megjelölése útján;

**adatmegsemmisítés:** az adatot tartalmazó adathordozó teljes fizikai megsemmisítése;

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

**adatfeldolgozó:** az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely - törvényben vagy az Európai Unió kötelező jogi aktusában meghatározott keretek között és feltételekkel - az adatkezelő megbízásából vagy rendelkezése alapján személyes adatokat kezel;

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

**profilalkotás:** személyes adat bármely olyan - automatizált módon történő - kezelése, amely az érintett személyes jellemzőinek, különösen a munkahelyi teljesítményéhez, gazdasági helyzetéhez, egészségi állapotához, személyes preferenciáihoz vagy érdeklődéséhez, megbízhatóságához, viselkedéséhez, tartózkodási helyéhez vagy mozgásához kapcsolódó jellemzőinek értékelésére, elemzésére vagy előrejelzésére irányul;

**címzett:** az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely részére személyes adatot az adatkezelő, illetve az adatfeldolgozó hozzáférhetővé tesz;

## 2. A személyes adatok kezelésének elvei

### 1. A személyes adatok kezelésének elvei

Az adatkezelő személyes adatokat, mint munkáltató és mint szerződéses partner kezel. A személyes adatok kezelésére vonatkozó elvek ezért egyrészt az EU rendelet, az Info tv és a Munka törvénykönyve alapján határozhatók meg.

#### a.) Célhoz kötöttség elve:

Személyes adat kizárólag **meghatározott, egyértelmű és jogszerű célból, valamely jog gyakorlása, vagy kötelezettség teljesítése érdekében** kezelhető. Az adatkezelésnek minden szakaszában meg kell felelnie az **adatkezelés céljának**, az adatkezelés a célokkal össze nem egyeztethető módon nem történhet. Az adatok felvételének és kezelésének **tisztességesnek és törvényesnek** kell lennie.

A munkavállalótól csak olyan adat közlése kérhető, amely **személyiségi jogát nem sérti**, és a **munkaviszony létesítése, teljesítése vagy megszűnése szempontjából lényeges**. A munkavállalóval szemben csak olyan alkalmassági vizsgálat alkalmazható, amelyet **munkaviszonyra vonatkozó szabály ír elő**, vagy amely munkaviszonyra vonatkozó szabályban **meghatározott jog gyakorlása, kötelezettség teljesítése érdekében szükséges**. ( Mt. 10§) **A munkavállaló személyiségi joga akkor korlátozható, ha a korlátozás a munkaviszony rendeltetésével közvetlenül összefüggő okból feltétlenül szükséges és a cél elérésével arányos. A személyiségi jog korlátozásának módjáról, feltételeiről és várható tartamáról, továbbá szükségességét és arányosságát alátámasztó körülményekről a munkavállalót előzetesen írásban tájékoztatni kell.**

A személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel helyreállítható. Az érintettel akkor helyreállítható a kapcsolat, ha az adatkezelő rendelkezik azokkal a technikai feltételekkel, amelyek a helyreállításhoz szükségesek.

Az adatkezelés során biztosítani kell az **adatok pontosságát, teljességét** és - ha az adatkezelés céljára tekintettel szükséges - **naprakészségét**, minden ésszerű intézkedést meg kell tenni annak érdekében, hogy az adatkezelés céljából pontatlan személyes adatok haladéktalanul törlésre vagy javításra kerüljenek. **Az adatok csak az adatkezelési cél eléréséhez szükséges ideig tárolhatóak.**

A személyes adatok kezelését **jogszerűen** és **tisztességesen**, valamint az érintett számára **átlátható módon** kell végezni.

Az adatkezelés célját az adatok rögzítését megelőzően, világosan és egyértelműen meg kell határozni.

A célnak kellően részletesnek kell lennie annak érdekében, hogy azonosíthatóak legyenek a szükséges adatkezelési műveletek és az alkalmazandó további garanciális szabályok.

A cél meghatározásának részletezettsége alapvetően az adatkezelés körülményeitől és a kezelt személyes adatok fajtáitól függ.

A munkáltatónak minden egyes adatkezelés esetében adatkezelési célonként külön-külön **meg kell határoznia azt a jogot, amelynek gyakorlásához szükséges valamely személyes adat kezelése, vagy azt a kötelezettséget, amelynek teljesítése szükségessé teszi az adatkezelést.**

A munkáltatónak minden adatkezeléséhez célt kell rendelnie. Azaz személyes adat csak akkor kezelhető, ha az lényeges, ha az adat kezelése nélkül a munkaviszony létesítése, fenntartása, megszűnése nem lenne lehetséges. A munkáltatónak az adatkezelései jogszerűségét elsősorban azzal kell alátámasztania, hogy minden adatkezelése vonatkozásában igazolni tudja az adatkezelés célját, és azt, hogy az adatkezelés a cél eléréséhez szükséges.

Mindezek alapján a munkáltató köteles a munkavállalóktól kért adatok körét előre oly módon meghatározni, hogy az adatok csakis a munkaviszony létesítéséhez, fenntartásához, megszűnéséhez kapcsolódjanak.

A **munkavállalókat tájékoztatni kell** arról, hogy a tőlük kért adatok, velük szemben alkalmazott vizsgálatok milyen információként szolgálhatnak a munkáltató számára.

Amennyiben az adatokon eltérő célokból végeznek műveleteket, akkor a célokat egyenként definiálni kell. Továbbá az **adatkezelésnek minden szakaszában meg kell felelnie az adott adatkezelési célnak, és tilos adatokat kezelni olyan újabb célból, amely összeegyeztethetetlen az eredetivel.**

## **b.)Szükségesség - arányosság elve**

A kezelt adatok körét a **szükséges mértékre** kell korlátozni- amely adat nem **szükséges** vagy **relaváns** az adatkezelési célhoz azt nem lehet kezelni.

Csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas. A személyes adat csak a cél megvalósulásához **szükséges mértékben és ideig** kezelhető.



## 2. A személyes adatok kezelésének jogalapja

A személyes adatok kezelése kizárólag akkor jogszerű, ha jogalapja megállapítható. A magyar és az uniós jogszabályi rendelkezések alapján különböző jogalapok alkalmazhatóak annak érdekében, hogy az adatkezelés jogszerű legyen, amelyek a következők lehetnek

- az érintett hozzájárulása
- szerződés teljesítése (amiben az érintett szerződő fél)
- az adatkezelőre vonatkozó jogi kötelezettség teljesítése
- az érintett személy létfontosságú érdekeinek védelme
- az adatkezelés közérdekű vagy az adatkezelőre ruházott jogosítvány gyakorlásának keretében történik
- az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges

### a) Az érintett hozzájárulása:

A hozzájárulás jogalapjának legfontosabb feltétele, hogy annak **önkéntesnek, azaz mindenfajta külső befolyástól mentesnek kell lennie és megfelelő tájékoztatásnak kell megelőznie**. A hozzájárulást valamennyi adatkezelési célhoz egyenként kell beszerezni. Az önkéntesség hiányában az adatkezelő nem rendelkezik megfelelő jogalappal az adatkezeléshez.

Az érintett hozzájárulására, mint jogalapra, a munkahelyi adatkezelések esetében csak kivételesen lehet hivatkozni, alapvetően akkor, amikor egyértelmű, hogy az adatkezelés során feltétel nélküli „előnyöket” szerez a munkavállaló, és nem érheti őt semmilyen hátrány az adatkezelés megtagadása esetén.

Ha a személyes adat felvételére az érintett hozzájárulásával került sor, az adatkezelő a felvett adatokat törvény eltérő rendelkezésének hiányában

- a) a rá vonatkozó jogi kötelezettség teljesítése céljából, vagy
- b) az adatkezelő vagy harmadik személy jogos érdekének érvényesítése céljából, ha ezen érdek érvényesítése a személyes adatok védelméhez fűződő jog korlátozásával arányban áll további külön hozzájárulás nélkül, valamint az érintett hozzájárulásának visszavonását követően is kezelheti.

Kétség esetén azt kell vélelmezni, hogy az érintett a hozzájárulását nem adta meg.

### b. Szerződés teljesítése

Természetes személyekkel, illetve jogi személyek természetes személy képviselőjével kötött szerződés esetében a szerződés megkötéséhez, illetve teljesítéséhez szükséges a szerződő

partner személyes adatainak kezelése. Mivel maga a szerződés a felek közötti konszenzust tükrözi ezért az adatkezelésnek ez egy jogszerű alapja.

Ha a hozzájáruláson alapuló adatkezelés célja az adatkezelővel írásban kötött szerződés végrehajtása, a szerződésnek tartalmaznia kell minden olyan információt, amelyet a személyes adatok kezelése szempontjából - e törvény alapján - az érintettnek ismernie kell, így különösen a kezelendő adatok meghatározását, az adatkezelés időtartamát, a felhasználás célját, az adatok továbbításának tényét, címzettjeit, adatfeldolgozó igénybevételének tényét. A szerződésnek félreérthetetlen módon tartalmaznia kell, hogy az érintett aláírásával hozzájárul adatainak a szerződésben meghatározottak szerinti kezeléséhez.

### **c. Jogi kötelezettség teljesítése**

Sok esetben magát az adatkezelést valamely jogszabályi előírás teljesítésére irányuló kötelezettség teszi szükségessé.

A munkahelyi adatkezelések egy jelentős része törvényi rendelkezésen alapul: vagy olyan törvényi előíráson, amely kötelezővé teszi az adatkezelést, vagy olyan jogszabályon, amely csupán lehetővé teszi az adatkezelést. Mindkét esetben előfordul, hogy az adott törvény az adatkezelés valamennyi körülményét szabályozza, de olyan jogszabály által nevesített adatkezelés is létezik, amelynél a törvény az adatkezelés részleteit, körülményeit nem határozza meg, azokat az adatkezelőre bízta.

Törvényen alapuló, kötelező adatkezelést széles körben rendelnek el az adókötelezettségre, társadalombiztosításra vonatkozó jogszabályok is. Ezen jogszabályok rendelkezései a munkáltatók és a munkavállalók számára kötelezettségként jelennek meg, vagyis ezek ténylegesen kötelező adatkezelések.

Ezen túlmenően a munkaviszonyra is irányadóak lehetnek olyan törvények, amelyek az adatkezelést a munkáltató számára lehetővé teszik.

### **d. érintett személy létfontosságú érdekeinek védelme**

Az érintett személy létfontosságú érdekei különösen az élet és testi épség védelme, vagyonának védelme.

#### **A Különleges adatok kezelése tilos kivéve ha**

- az érintett kifejezett hozzájárulása,
- a saját vagy más személy létfontosságú érdekeinek védelméhez,
- az adatkezelés az adatkezelőnek vagy az érintettnek a foglalkoztatása érdekében szükséges
- az adatkezelés valamely politikai, világnézeti, vallási vagy szakszervezeti célú alapítvány, egyesület vagy bármely más nonprofit szervezet megfelelő garanciák mellett végzett jogszerű tevékenysége keretében történik
- az adatkezelés olyan személyes adatokra vonatkozik, amelyeket az érintett kifejezetten nyilvánosságra hozott,
- az adatkezelés jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez szükséges, vagy amikor a bíróságok igazságszolgáltatási feladatkörükben járnak el,
- az adatkezelés jelentős közérdek miatt szükséges,
- az adatkezelés megelőző egészségügyi vagy munkahelyi egészségügyi célokból, a munkavállaló munkavégzési képességének felmérése, orvosi diagnózis felállítása,

egészségügyi vagy szociális ellátás vagy kezelés nyújtása, illetve egészségügyi vagy szociális rendszerek és szolgáltatások irányítása érdekében szükséges

Ha az érintett cselekvőképtelensége folytán vagy más elháríthatatlan okból nem képes hozzájárulását megadni, akkor a saját vagy más személy létfontosságú érdekeinek védelméhez, valamint a személyek életét, testi épségét vagy javait fenyegető közvetlen veszély elhárításához vagy megelőzéséhez szükséges mértékben a hozzájárulás akadályainak fennállása alatt az érintett személyes adatai kezelhetők.

A 16. életévét betöltött kiskorú érintett hozzájárulását tartalmazó jognyilatkozatának érvényességéhez törvényes képviselőjének beleegyezése vagy utólagos jóváhagyása nem szükséges.

#### **e. A jogos érdeken alapuló adatkezelés**

A jogos érdeken alapuló adatkezelés esetében pontosan meg kell határozni azt az érdeket, ami az adatkezelést indokolja. Ilyen érdek lehet különösen

- élet és testi épség védelme, **különös tekintettel az emberi életre veszélyes járványhelyzetben folytatott védekezés**
- vagyonvédelem
- csalások, bűncselekmények megelőzése
- közvetlen üzletszerzés
- munkaszervezés
- hatékonyság növelés
- technikai eszközök működőképességének ellenőrzése
- technológia betartásának ellenőrzése
- állatjóléti ellenőrzések

Az Adatvédelmi Irányelv értelmében személyes adat kezelhető abban az esetben is, ha a munkahelyi adatkezelés a munkáltató – kivételesen harmadik fél – jogos érdekének érvényesítéséhez szükséges, kivéve, ha ennél az érdekeknél magasabb rendűek a munkavállalók személyes adatai védelméhez és a magánéletük tiszteletben tartásához való joguk.

A jogalap egyik fő jellemzője az, hogy ez a munkavállalók hozzájárulásától függetlenül jogszerűvé teheti a munkáltató adatkezelését, feltéve, ha a munkáltató jogos érdeke arányosan korlátozza a munkavállalók személyes adatok védelméhez való jogát, magánszféráját.

A jogalap alkalmazása során a munkáltatónak két követelményre kell figyelemmel lennie. Egyrészt ezen jogalap alkalmazásakor a magyar jogszabályi előírásokat, így különösen az Mt. és az Infotv. rendelkezéseit kell alapul vennie. Másrészt ezzel egyidejűleg el kell végeznie az érdekmérlegelési tesztet. Az érdekmérlegelési tesztet az alábbiak figyelembe vételével kell elvégezni:

- milyen szempontok alapján lehet meghatározni a munkáltatói jogos érdeket,
  - mire kell a munkáltatónak figyelemmel lennie az érintetti érdekek, jogok meghatározása során,
  - melyek az érdekmérlegelési teszt elvégzése során megfontolandó kulcsfontosságú tényezők,
  - melyek lehetnek például az adatkezelők által alkalmazott olyan intézkedések, amelyek biztosítják az érintettek magánszférájának és személyes adatainak védelmét.
- Az érdekmérlegelési teszt elvégzése során a munkáltatónak számos szempontra figyelemmel kell lennie, ezért az érdekmérlegelést több lépcsőben kell végrehajtani.
- *1. lépés:* a munkáltatónak a tervezett adatkezelés megkezdése előtt át kell tekintenie, 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 munkáltatói jogos érdek lehető legpontosabb meghatározása (így különösen az Mt. 10. § (1) bekezdésének figyelembe vételével).
  - *3. lépés:* annak meghatározása, hogy mi az adatkezelés célja, milyen személyes adatok, meddig tartó adatkezelését igényli a jogos érdek.
  - *4. lépés:* annak meghatározása, hogy a munkavállalóknak mik lehetnek az érdekeik az adott adatkezelés vonatkozásában
  - *5. lépés:* annak meghatározása, hogy miért korlátozza arányosan a munkáltatói jogos érdek – és az ennek alapján végzett adatkezelés a munkavállalói jogokat, várakozásokat.

Az érdekmérlegelésen alapuló munkahelyi adatkezelések esetében többek között az alábbi garanciák biztosíthatják az adatkezelés szükségesség-arányosságát:

- *A fokozatosság elvének érvényesülése.* Ennek a garanciának elsődlegesen a munkáltatói ellenőrzésekkel együtt járó adatkezelések esetén van jelentősége. A munkáltatónak a munkavállalók munkaviszonnnyal összefüggő magatartásának ellenőrzése körében lehetőleg olyan módszert kell választania, amely nem jár együtt személyes adat kezelésével. Ha nincs ilyen, akkor a magánszférát legkevésbé korlátozó módszert kell alkalmaznia, amelynek nyomán korlátozott körben ismer meg személyes adatokat.
- *A munkavállaló jelenlétének biztosítása.* Ugyancsak a munkáltatói ellenőrzések keretében van szerepe ezen garanciának. Amennyiben az ellenőrzés körülményei nem zárják ki ennek lehetőségét, akkor biztosítani kell, hogy a munkavállaló jelen lehessen az ellenőrzés

## **A koronavírus terjedésére tekintettel**

- 1. Az a munkavállaló, akinél, vagy akinek családtagjánál koronavírus fertőzés veszélye áll fenn, illetve akinél koronavírus fertőzést diagnosztizálnak haladéktalanul köteles ezt telefonon a munkahelyi vezetőjének bejelenteni.  
A munkahelyi vezetők kötelesek a hozzájuk érkezett bejelentéseket haladéktalanul továbbítani a főágazatvezető és a vezérigazgató felé, valamint kötelesek a lehetséges fertőtlenítéseket elrendelni és a szükséges óvintézkedéseket megtenni.**
- 2. A társaság valamennyi telephelyén a munkavállalók a munka megkezdése előtt kötelesek a munkahelyi vezetőnél jelentkezni, nyilatkozni arra vonatkozóan, hogy**

**fertőzött személlyel nem kerültek kapcsolatba, illetve betegség jeleit nem mutatják. A munkahelyi vezető a nyilatkozatot követően elvégzi a testhőmérséklet ellenőrzést. Az ellenőrzés eredményétől függően a munkahelyi vezető dönt arról, hogy a munkavállaló végezhet-e munkát.**

**A munkavállalók kötelesek a munkahelyi vezetőket értesíteni amennyiben a közvetlen környezetükben (szűkebb és tágabb család, rokonság, szomszéd, barát) lázas beteg, koronavírusos megbetegedés, önkéntes vagy hatósági karantén van.**

**A munkáltató a vírus elleni védekezés során tudomására jutott egészségi adatokat kizárólag a többi munkavállaló életének és testi épségének megóvása, illetve a munkavégzés megszervezése érdekében használhatja fel.**

### **3. A személyes adatok biztonságának követelménye**

A Társaság köteles az adatkezelési műveleteket úgy megtervezni és végrehajtani, hogy az biztosítsa az érintettek magánszférájának védelmét.

A Társaság, illetve tevékenységi körében az adatfeldolgozást végző személy köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek az adatvédelmi törvény valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.

A személyes adatok kezelését oly módon kell végezni, hogy **megfelelő technikai vagy szervezési** intézkedések alkalmazásával **biztosítva legyen a személyes adatok megfelelő biztonsága**

- az adatok jogosulatlan vagy jogellenes kezelésével
- véletlen elvesztésével
- megsemmisítésével vagy
- károsodásával szembeni védelmet is ideértve

**Az adatkezelés során az adatkezelő minden olyan technikai és szervezési intézkedést megtesz melyek az adatvédelmi elvek megvalósítását, és az adatkezelés során szükséges garanciák érvényesülését biztosítják.**

Az adatokat megfelelő intézkedésekkel védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen.

A különböző nyilvántartásokban elektronikusan kezelt adatállományok védelme érdekében megfelelő technikai megoldással biztosítani kell, hogy a nyilvántartásokban tárolt adatok közvetlenül ne legyenek összekapcsolhatók és az érintetthez rendelhetők.

Az adatkezelőnek és az adatfeldolgozónak az adatok biztonságát szolgáló intézkedések

meghatározásakor és alkalmazásakor tekintettel kell lenni a technika mindenkori fejlettségére.

Több lehetséges adatkezelési megoldás közül azt kell választani, amely a személyes adatok magasabb szintű védelmét biztosítja, kivéve, ha az aránytalan nehézséget jelentene az adatkezelőnek.

#### **4. Az érintett személyek jogai**

Az érintett személyeknek az adatkezeléssel kapcsolatban az alábbi jogai vannak:

- Átlátható tájékoztatáshoz, kommunikációhoz való jog
- az adatkezelőnek elő kell segítenie, hogy az érintett a jogait gyakorolni tudja
- hozzáférési jog
- helyesbítéshez való jog
- törléshez való jog
- adatkezelés korlátozásához való jog
- adathordozhatósághoz való jog
- tiltakozáshoz való jog
- automatizált döntés alóli mentesség joga
- adatvédelmi incidensről való tájékoztatás joga
- panasztétel joga (hatósági jogorvoslathoz való jog)
- bírósági jogorvoslathoz való jog (hatósággal, illetve adatkezelővel szemben)

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 nevről, 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.

Az adatkezelő az adatvédelmi incidenssel kapcsolatos intézkedések ellenőrzése, valamint az érintett tájékoztatása céljából nyilvántartást vezet, amely tartalmazza az érintett személyes adatok körét, az adatvédelmi incidenssel érintettek körét és számát, az adatvédelmi incidens időpontját, körülményeit, hatásait és az elhárítására megtett intézkedéseket, valamint az adatkezelést előíró jogszabályban meghatározott egyéb adatokat.

Az adatkezelő az adattovábbítás jogszerűségének ellenőrzése, valamint az érintett tájékoztatása céljából adattovábbítási nyilvántartást vezet, amely tartalmazza az általa kezelt személyes adatok továbbításának időpontját, az adattovábbítás jogalapját és címzettjét, a továbbított személyes adatok körének meghatározását, valamint az adatkezelést előíró jogszabályban meghatározott egyéb adatokat.

Az adatkezelő köteles a kérelem benyújtásától számított legrövidebb idő alatt, legfeljebb azonban 25 napon belül, közérthető formában, az érintett erre irányuló kérelmére írásban megadni a tájékoztatást.

Az adatkezelő megjelöli az általa kezelt személyes adatot, ha az érintett vitatja annak helyességét vagy pontosságát, de a vitatott személyes adat helytelensége vagy pontatlansága

nem állapítható meg egyértelműen.

A helyesbítésről, a zárolásról, a megjelölésről és a törlésről az érintettet, továbbá mindazokat értesíteni kell, akiknek korábban az adatot adatkezelés céljára továbbították. Az értesítés mellőzhető, ha ez az adatkezelés céljára való tekintettel az érintett jogos érdekét nem sérti.

Ha az adatkezelő az érintett helyesbítés, zárolás vagy törlés iránti kérelmét nem teljesíti, a kérelem kézhezvételét követő 25 napon belül írásban vagy az érintett hozzájárulásával elektronikus úton közli a helyesbítés, zárolás vagy törlés iránti kérelem elutasításának ténybeli és jogi indokait. A helyesbítés, törlés vagy zárolás iránti kérelem elutasítása esetén az adatkezelő tájékoztatja az érintettet a bírósági jogorvoslat, továbbá a Hatósághoz fordulás lehetőségéről.

## **5. Az érintett előzetes tájékoztatásának követelménye**

### **Az előzetes tájékoztatás követelménye**

**Infotv. 20. § (1)-(2) bekezdés** Az érintettel az adatkezelés megkezdése előtt közölni kell, hogy az adatkezelés hozzájáruláson alapul vagy kötelező. Az érintettet az adatkezelés megkezdése előtt egyértelműen és részletesen tájékoztatni kell az adatai kezelésével kapcsolatos minden tényről, így különösen az adatkezelés céljáról és jogalapjáról, az adatkezelésre és az adatfeldolgozásra jogosult személyéről, az adatkezelés időtartamáról, arról, ha az érintett személyes adatait az adatkezelő a 6. § (5) bekezdése alapján kezeli, illetve arról, hogy kik ismerhetik meg az adatokat. A tájékoztatásnak ki kell terjednie az érintett adatkezeléssel kapcsolatos jogaira és jogorvoslati lehetőségeire is.

**Mt 9 § A munkavállaló személyiségi joga akkor korlátozható, ha a korlátozás a munkaviszony rendeltetésével közvetlenül összefüggő okból feltétlenül szükséges és a cél elérésével arányos. A személyiségi jog korlátozásának módjáról, feltételeiről és várható tartamáról, továbbá szükségességét és arányosságát alátámasztó körülményekről a munkavállalót előzetesen írásban tájékoztatni kell.”**

**Mt 10. § (1) A munkáltató a munkavállalótól olyan nyilatkozat megtételét vagy személyes adat közlését követelheti, amely a munkaviszony létesítése, teljesítése, megszűnése (megszüntetése) vagy e törvényből származó igény érvényesítése szempontjából lényeges.**

**(2) A munkáltató, az üzemi tanács, a szakszervezet e törvény Harmadik Részében meghatározott jogának gyakorlása vagy köteletségének teljesítése céljából nyilatkozat megtételét vagy adat közlését követelheti.**

**(3) Az (1) és (2) bekezdés alapján okirat bemutatása követelhető.**

**(4) A munkavállalóval szemben olyan alkalmassági vizsgálat alkalmazható, amelyet munkaviszonyra vonatkozó szabály ír elő, vagy amely munkaviszonyra vonatkozó szabályban meghatározott jog gyakorlása, kötelezettség teljesítése érdekében szükséges.**

**(5) A munkáltató az (1)-(4) bekezdésen alapuló adatkezeléséről az érintettet írásban tájékoztatja.”**

**Mt. 11. § (1) A munkavállaló biometrikus adata az érintett azonosítása céljából abban az esetben kezelhető, ha ez valamely dologhoz vagy adathoz történő olyan jogosulatlan hozzáférés megakadályozásához szükséges, amely**

**a) a munkavállaló vagy mások élete, testi épsége vagy egészsége, vagy**

**b) törvényben védett jelentős érdek súlyos vagy tömeges, visszafordíthatatlan sérelmének a veszélyével járna.**

(2) Az (1) bekezdés b) pontja alkalmazásában jelentős védett érdek különösen

- a) a legalább „Bizalmas!” minősítési szintű minősített adatok védelméhez,
- b) a lőfegyver, lőszer, robbanóanyag őrzéséhez,
- c) a mérgező vagy veszélyes vegyi vagy biológiai anyagok őrzéséhez,
- d) a nukleáris anyagok őrzéséhez,
- e) a Btk. szerint legalább különösen nagy vagyoni érték védelméhez fűződő érdek.

(3) A munkáltató a munkavállaló vagy a munkáltatóval munkaviszonyt létesíteni szándékozó személy bűnügyi személyes adatát annak vizsgálata céljából kezelheti, hogy törvény vagy a (4) bekezdésben foglaltak szerint a munkáltató a betölteni kívánt vagy a betöltött munkakörben nem korlátozza vagy nem zárja-e ki a foglalkoztatást.

(4) A (3) bekezdés szerinti korlátozó vagy kizáró feltételt a munkáltató akkor határozhatja meg, ha az adott munkakörben az érintett személy foglalkoztatása

- a) a munkáltató jelentős vagyoni érdeke,
- b) törvény által védett titok, vagy
- c) a (2) bekezdés b)-d) pontja szerinti törvény által védett érdek sérelmének veszélyével járna.

(5) A munkáltató a bűnügyi személyes adat kezelését megalapozó (4) bekezdés szerinti korlátozó vagy kizáró feltételt, és a bűnügyi személyes adat kezelésének feltételeit előzetesen írásban meghatározza.

**Mt. 11/A. § (1)** A munkavállaló a munkaviszonnal összefüggő magatartása körében ellenőrizhető. Ennek keretében a munkáltató technikai eszközt is alkalmazhat, erről a munkavállalót előzetesen írásban tájékoztatja.

(2) A munkavállaló a munkáltató által a munkavégzéshez biztosított információtechnológiai vagy számítástechnikai eszközt, rendszert (a továbbiakban: számítástechnikai eszköz) - eltérő megállapodás hiányában - kizárólag a munkaviszony teljesítése érdekében használhatja.

(3) A munkáltató ellenőrzése során a munkaviszony teljesítéséhez használt számítástechnikai eszközön tárolt, a munkaviszonnal összefüggő adatokba tekinthet be.

(4) A (3) bekezdés szerinti ellenőrzési jogosultság szempontjából munkaviszonnal összefüggő adatnak minősül a (2) bekezdésben meghatározott korlátozás betartásának ellenőrzéséhez szükséges adat.

(5) A (3) bekezdést alkalmazni kell, ha a felek megállapodása alapján a munkavállaló a munkaviszony teljesítése érdekében saját számítástechnikai eszközt használ.

Írásbelinek kell tekinteni a jognyilatkozatot,) „b) a 9. § (2) bekezdésében, a 10. § (5) bekezdésében, a 11. § (5) bekezdésében, a 11/A. § (1) bekezdésében, a 93. § (4) bekezdésében, a 97. § (4) bekezdésében, a 108. § (1) bekezdésében, a 110. § (5) és (6) bekezdésében, a 138. § (4) bekezdésében és a 193. § (2) bekezdésében meghatározott esetekben akkor is, ha azt a helyben szokásos és általában ismert módon közzéteszik.

Kötelező adatkezelés esetén a tájékoztatás megtörténhet az információkat tartalmazó jogszabályi rendelkezésekre való utalással is.

## 6. Tiltakozás személyes adat kezelése ellen



Az érintett tiltakozhat személyes adatának kezelése ellen,

a) 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;

b) ha a személyes adat felhasználása vagy továbbítása közvetlen üzletszerzés, közvélemény-kutatás vagy tudományos kutatás céljára történik; valamint

c) 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, és 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 adatkezelőnek a meghozott döntésével nem ért egyet, illetve, ha az adatkezelő a határidőt elmulasztja, az érintett - a döntés közlésétől, illetve a határidő utolsó napjától számított 30 napon belül - bírósághoz fordulhat.

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.

## **7. A társaság által kezelt személyes adatok köre:**

### **Adatkezelés célja:**

A társaság csak olyan személyes adatokat kezel, melyek tevékenységének ellátásához, feladatainak teljesítéséhez szükségesek. Az adatkezelés célja alapján az alábbi adatokat különbözteti meg a társaság:

- munkaviszony létesítéséhez, teljesítéséhez fenntartásához (foglalkoztatáshoz), megszüntetéséhez kapcsolódó adatok , **illetve a munka törvénykönyvéből származó igény érvényesítése szempontjából lényeges**
- társadalombiztosítási kifizetésekhez kapcsolódó adatok (TB kifizető hely)
- törvényi előírások teljesítése
- földterületek bérletéhez kapcsolódó adatok
- szerződések létesítése, teljesítése, pénzügyi kapcsolatokhoz szükséges adatok
- vagyonvédelemhez kapcsolódó adatok
- önkéntes pénztári belépéshez, tagsághoz kapcsolódó adatok
- kollektív szerződéses juttatások biztosításához szükséges adatok
- továbbképzésekhez szükséges adatok
- társaság jogos érdekének biztosításához szükséges adatok

### **Érintettek kategóriái:**

- munkavállalók, munkára jelentkezők, tanulók
- munkavállalók családtagjai
- földtulajdonosok, föld bérbeadók,
- szerződő partnerek, beszállítók, vevők,
- a társaság területére látogatók,

### **Személyes adatok kategóriái:**

- név, születéskori név
- születési hely, idő
- anyja neve
- lakcím, tartózkodási hely
- állampolgárság
- adóazonosító jel
- személyi azonosító szám (kizárólag ingatlannyilvántartáshoz kapcsolódó partnereknél)
- nyugdíjas törzsszám
- nyugdíj típusa, összege
- TAJ szám
- iskolai végzettség, bizonyítvány
- jogosítvány típusa száma, kategóriája
- családi állapot,
- gyermekek száma, neve, adóazonosítója, TAJ száma
- házastárs neve, adóazonosítója, TAJ száma,
- munka alkalmassági egészségügyi állapot,
- szakszervezeti tagság,
- vállalkozói igazolvány szám, nyilvántartási szám,
- östermelői igazolvány szám, adószám értékesítési betétlap,
- regisztrációs szám,
- székhely, telephely,
- adószám, közösségi adószám, csoport adószám,
- pénzforgalmi adózás jelölése,
- bankszámlaszám,
- előző munkahely- TB kiskönyv,
- előző munkahelyek igazolásai,
- fennálló tartozások, gyerektartás,
- tulajdonát képező ingatlan adatai,
- tulajdoni, haszonélvezeti arány,
- munkaképesség csökkenésére vonatkozó adatok,
- telefonszám, email cím,
- kamera felvételek,
- GPS adatok,

A társaság a munkavállalók és szerződéses partnerek személyes adatait tartalmazó okmányokról másolatot készít, illetve szkennelt formában tárolja azokat.

### **Címzettek kategóriái:**

- NAV
- foglalkozás egészségügyi szolgálat
- önkéntes nyugdíjpénztár
- nyugdíj és egészségbiztosítási pénztár, igazgatóság
- bíróság
- végrehajtók,
- önkormányzatok
- földhivatal
- kamarák
- bankok
- iskolák, képző helyek
- kollektív szerződés alapján nyújtott juttatás szolgáltatója
- NEXON bérprogram üzemeltetője

#### **Törlési határidők:**

- önéletrajzok, pályázatok- elbírálást követően törlésre kerülnek.
- munkaviszonyhoz kapcsolódó adatok- 60 év
- társadalombiztosításhoz kapcsolódó adatok- 60 év
- GPS adatok- maximum 6 hónap
- kamera felvételek- maximum 6 hónap

**A kezelt adatokra vonatkozó részletes információkat az 1. sz melléklet tartalmazza.**

### **8. Az adattovábbítás szabályai**

Az Infotv. 3. § 13. pontja értelmében adattovábbításnak minősül az, amikor személyes adatot meghatározott harmadik személy számára hozzáférhetővé tesznek. Az Infotv. 3. § 22. pontja alapján harmadik személy az adatkezelőn, az érintetten és az adatfeldolgozón kívül minden más személy és szervezet. A munkaviszonyban az érintett a munkavállaló, az adatkezelő a munkáltató, és minden, rajtuk kívüli személy harmadik személynek minősül, így például harmadik személynek minősülnek a munkáltatóval egy vállalatcsoportban lévő más vállalatok is. Ebből fakadóan adattovábbításnak tekinthető az is, amikor a munkáltató egy közös adatbázisba tölti fel a munkavállalók személyes adatait, amely adatbázishoz más adatkezelők (más leányvállalatok, az anyavállalat) is hozzáférhet.

#### **Adattovábbítás külföldre**

##### **a. Adattovábbítás az EGT-n belül**

Az Infotv. 8. § (4) bekezdése szerint az EGT-államba irányuló adattovábbítást úgy kell tekinteni, mintha Magyarország területén belüli adattovábbításra kerülne sor. Az Infotv. rendelkezése természetesen irányadó a munkáltatók adattovábbításaira is, azokkal a korlátozásokkal, amelyeket az Mt. tartalmaz.

Az Mt. 10. § (2) bekezdés alapján a munkáltató a munkavállalóra vonatkozó adatot harmadik személlyel csak törvényben meghatározott esetben vagy a munkavállaló hozzájárulásával közzéteheti.

## **b. Adattovábbítás az EGT-n kívülre**

Amennyiben nem EGT-államban, azaz harmadik országban honos adatkezelő vagy adatfeldolgozó részére történik az adatok továbbítása, akkor arra elsődlegesen az Infotv. 8. § (1)- (2) bekezdésében megjelölt esetekben kerülhet sor.

Ez alapján – a munkahelyi adatkezelések sajátosságaira is figyelemmel – két esetkör alapján lehet harmadik országban honos munkáltató (adatkezelő, adatfeldolgozó) számára adatot továbbítani:

1. Az első esetkör az érintett kifejezett hozzájárulásán alapuló adattovábbítás. A munkáltatótól elvárható, hogy a munkavállalók személyes adatait csak megfelelő védelmet nyújtó harmadik országokba továbbítsa, vagy az Infotv. és az uniós jogszabályok által rögzített más módon biztosítsa a megfelelő szintű védelmet az adattovábbítással összefüggésben.

2. A második esetkör az érintett kifejezett hozzájárulásának hiányában, ha az alábbi konjunktív feltételek teljesülnek:

a. az Infotv. hatálya alá tartozó adatkezelő (az adattovábbító szervezet) az Infotv. vagy az Adatvédelmi Irányelv által elismert jogalappal rendelkezik az adatkezeléshez, és

b. a harmadik országban a személyes adatok megfelelő szintű védelme biztosított, mivel:

i. az adattovábbítással összefüggésben az Európai Unió kötelező erejű jogi aktust fogadott el, vagy

ii. az adattovábbításra vonatkozó kötelező szervezeti szabályozást (angol nyelvű elnevezéssel: *binding corporate rules*; a továbbiakban: BCR) a Hatóság jóváhagyta. A BCR lehetővé teszi, hogy egy multinacionális vállalat Infotv. hatálya alá tartozó tagja személyes adatokat továbbítsa az EGT-térségen kívüli országokban található tagjai részére oly módon, hogy az adattovábbítás megfeleljen mind az uniós, mind a magyar adatvédelmi követelményeknek.

## **9. Az adatvédelmi incidens**

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.

Adatvédelmi incidensek különösen:

- céges laptop, mobiltelefon elvesztése
- személyes adatok nem biztonságos tárolása
- adatok nem biztonságos továbbítása
- személyes adatokat tartalmazó iratok illetéktelen másolása továbbítása
- szerver elleni támadások, honlap feltörése

Az adatvédelmi incidenst az adatkezelő indokolatlan késedelem nélkül legkésőbb a tudomására jutást követő 72 órán belül köteles bejelenteni a felügyeleti hatóságnak (NAIH) kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira nézve.

Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár az adatkezelőnek késedelem nélkül tájékoztatnia kell az érintett személyt is.

Az adatkezelő az adatvédelmi incidensekről nyilvántartást vezet.

## 10. Egyes speciális munkahelyi adatkezelések

### a. Az álláspályázatra jelentkezés

#### A pályázatok, önéletrajzok megőrzése

Az Infotv. 4. § (1)-(2) bekezdése alapján az önéletrajzok, pályázatok esetében az adatkezelés célja az, hogy a meghirdetett munkakört betöltsék. Ennek megfelelően, ha a munkáltató a jelentkezők közül kiválasztott egy személyt a meghirdetett állásra, akkor megszűnt az adatkezelés célja, és – az Infotv. 17. § (2) bekezdés d) pontja alapján – a ki nem választott jelentkezők személyes adatait törölni kell. Ezzel egyidejűleg fennáll a törlési kötelezettség abban az esetben is, ha az érintett még a jelentkezés során meggondolja magát, visszavonja pályázatát. Az Infotv. 17. § (2) bekezdés d) pontja értelmében: *„a személyes adatot törölni kell, ha (...) az adatkezelés célja megszűnt (...)”*

A munkáltató alapvetően csak az érintett kifejezett, egyértelmű és önkéntes hozzájárulása alapján őrizheti meg a pályázatokat, feltéve, ha azok megőrzésére az Infotv. 4. § (1)-(2) bekezdésével összhangban álló adatkezelési célja elérése érdekében szükség van.

#### A pályázati anyagok kezelésével kapcsolatos egyéb adatvédelmi követelmények

A jelentkezők információs önrendelkezési jogát az biztosítja a legmagasabb szinten, ha tájékoztatást kapnak arról is, ha a munkáltató nem őt választotta az adott állásra.

Az Infotv. szabályozása alapján személyes adatnak minősül az adatból levont, az érintettre vonatkozó következtetés is. Ennek megfelelően, ha a munkáltató bármilyen feljegyzést készít a pályázóról, akkor az is a pályázó személyes adatának minősül. Ezzel kapcsolatban két adatvédelmi követelményt szükséges szem előtt tartani:

- erre is kiterjed az érintett tájékoztatáshoz való joga, vagyis, hogy megismerje, a munkáltató milyen következtetéseket vont le a pályázati anyagával összefüggésben.
- a munkáltatónak törölnie kell az ilyen természetű, az érintettre levont következtetéseket tartalmazó feljegyzéseket is.

### b. Alkalmassági vizsgálatok

Az Mt. 10. § (4) bekezdése alapján a munkavállalókkal szemben olyan alkalmassági vizsgálat alkalmazható:

- **amelyeket munkaviszonyra vonatkozó szabály ír elő.**
- **amely a munkaviszonyra vonatkozó szabályban meghatározott jog gyakorlása, kötelezettség teljesítése érdekében szükséges.**

Részletesen tájékoztatni kell a munkavállalókat többek között arról, hogy az alkalmassági vizsgálat milyen készség, képesség felmérésére irányul, a vizsgálat milyen eszközzel, módszerrel történik. Amennyiben jogszabály írja elő a vizsgálat elvégzését, akkor tájékoztatni kell a munkavállalókat erről.

Kizárólag a vizsgált munkavállalók, illetve a vizsgálatot végző szakember ismerhetik meg az eredményeket, kivéve az alkalmassági minősítést.

#### A koronavírus terjedésére tekintettel

**A munkára jelentkező személy nyilatkozni köteles saját és hozzátartozói egészségi állapotára és esetleges külföldi utazásaira vonatkozóan.**

**Az a munkavállaló, akinél, vagy akinek családtagjánál koronavírus fertőzés veszélye áll fenn, illetve akinél koronavírus fertőzést diagnosztizálnak haladéktalanul köteles ezt telefonon a munkahelyi vezetőjének bejelenteni.**

**A munkahelyi vezetők kötelesek a hozzájuk érkezett bejelentéseket haladéktalanul továbbítani a főágazatvezető és a vezérigazgató felé, valamint kötelesek a lehetséges fertőtlenítéseket elrendelni és a szükséges óvintézkedéseket megtenni.**

**A társaság valamennyi telephelyén a munkavállalók a munka megkezdése előtt kötelesek a munkahelyi vezetőnél jelentkezni, nyilatkozni arra vonatkozóan, hogy fertőzött személlyel nem kerültek kapcsolatba, illetve betegség jeleit nem mutatják. A munkahelyi vezető a nyilatkozatot követően elvégzi a testhőmérséklet ellenőrzést. Az ellenőrzés eredményétől függően a munkahelyi vezető dönt arról, hogy a munkavállaló végezhet-e munkát.**

**A munkavállalók kötelesek a munkahelyi vezetőket értesíteni amennyiben a közvetlen környezetükben (szűkebb és tágabb család, rokonság, szomszéd, barát) lázas beteg, koronavírusos megbetegedés, önkéntes vagy hatósági karantén van.**

**A munkáltató a vírus elleni védekezés során tudomására jutott egészségi adatokat kizárólag a többi munkavállaló életének és testi épségének megóvása, illetve a munkavégzés megszervezése érdekében használhatja fel.**

### **c. A munkavállalók feddhetetlen előéletének igazolása**

A hatósági erkölcsi bizonyítvány, mint jogintézmény célja többek között az, hogy a munkavállaló a munkáltató előtt erkölcsi alkalmasságát az adott munkakörrel kapcsolatosan igazolja. Erre az érintettet a munkaviszony létesítése előtt, a felvételi eljárás során, illetőleg a munkaviszony fennállása alatt is felszólíthatja a munkáltató, amennyiben az erkölcsi alkalmasság igazolása valamely **jogszabályban, vagy a munkáltató által meghatározottak** szerint, az adott munkakör betöltéséhez valóban elengedhetetlen.

### **d. A munkavállalók munkaviszonnal összefüggő magatartásának ellenőrzése**

#### **Munkahelyi kamerás megfigyelés**

Jogszabály négy esetben teszi lehetővé az elektronikus megfigyelőrendszer alkalmazását:

- az emberi élet, testi épség, személyi szabadság védelme,
- a veszélyes anyagok őrzése,
- az üzleti, fizetési, bank- és értékpapírtitok védelme,
- vagyónvédelem.

A célhoz kötött adatkezelés elvéből fakadóan tehát munkahelyen elektronikus megfigyelőrendszert alkalmazni elsődlegesen ezen célokból lehet, illetve a rögzített felvételek is ezen célokból használhatók fel. Amennyiben a munkáltató más célból szeretné alkalmazni a kamerás megfigyelést, akkor ott igazolnia kell azt a jogos érdeket, amely szükségessé teszi a kamera alkalmazását.

Az elektronikus megfigyelőrendszerek alkalmazhatóságának fontos feltétele, hogy semmiképp sem lehet kamerát elhelyezni olyan helyiségben, amelyben a megfigyelés az emberi méltóságot sértheti, így különösen az öltözőkben, zuhanyzóknak, az illemlhelyiségekben vagy például orvosi szobában, váróban.

A munkáltató elektronikus megfigyelőrendszert kizárólag a saját tulajdonában (vagy a használatában) álló épületrészek, helyiségek és területek, illetőleg az ott történt események megfigyelésére alkalmazhat, közterület megfigyelésére azonban nem.

Az elektronikus megfigyelőrendszer által rögzített felvételek tárolásának időtartama maximum 6 hónap.

- az adatkezelés jogalapja: élet és testi épség védelme, vagyónvédelem, állatjóléti feltételeknek való megfelelés,
- a felvétel tárolásának helyét is időtartamát az adatok megismerésére jogosult személyek körét a melléklet tartalmazza,

• a felvételek visszánézésére a mellékletben meghatározott személyek jogosultak, amennyiben a jogalap sérelme feltételezhető. A munkáltató a felvételeket a jogalpnál meghatározott ellenőrzéseken túl az Mt 11§ (2) bekezdésében foglaltak ellenőrzésére is felhasználhatja, vagyon elleni cselekmények esetében pedig a nyomozó hatóságoknak továbbíthatja.

• a munkavállalót megilleti a kamera felvételek visszánézésénél való részvétel joga, a kamera felvétel tárolási időt követő törlésének követelésére való jog, valamint a továbbításról való tájékoztatás joga. A jogok megsértése esetén a munkavállalók az általános adatvédelmi jogorvoslatra jogosultak.

### **A munkáltató által a munkavállaló rendelkezésére bocsátott e-mail fiók használatának ellenőrzése**

A társaság a vezetők, középvezetők illetve adminisztratív munkavállalók részére céges email fiókot hoz létre. A munkavállalók az email fiókot magán célra is használhatják. Az e-mail fiók használatát a munkáltató nem ellenőrzi.

A „céges e-mail fiók” esetleges ellenőrzése illetve a munkaállomás átadása esetében a **munkáltatói jogos érdek** lesz az adatkezelés jogalapja. Ezen ellenőrzés esetében kiemelt figyelmet kell fordítani az célhoz kötött adatkezelés elvén és a szükségesség-arányosság követelményén túl az érintettek magánszférájára is, hiszen adott esetben különféle, a munkaviszonyhoz nem kapcsolódó személyes adat is a munkáltató tudomására juthat, illetve vele munkaviszonyban nem álló személyek (az e-mailek küldői vagy címzettjei) adatait is megismerheti. A munkáltatónak az email fiók használatának ellenőrzése illetve átadása előtt közölnie kell a munkavállalókkal, hogy milyen érdeke miatt kerül sor a munkáltatói intézkedésre. A munkavállaló az ellenőrzés illetve az átadás előtt a magán jellegű emailokat jogosult törölni.

Az ellenőrzés első lépéseként az e-mail cím és a levél tárgyának az ellenőrzésére kerül sor.

A magánjellegű levelekkel kapcsolatban szükséges kiemelni azt is, hogy az ilyen e-mailek tartalmát a munkáltató nem jogosult megismerni

Az e-mail fiók használatának ellenőrzésénél, átadásánál biztosítani kell a munkavállaló jelenlétét. A munkáltatói ellenőrzés e formájánál ugyanis a munkavállaló és harmadik személyek különböző személyes adatai lehetnek benne a levelezőrendszerben, amelyek megismerésére a munkáltató nem jogosult. Az ellenőrzést megelőzően a munkáltatónak részletes tájékoztatást kell biztosítania a munkavállalók számára. A tájékoztatásban a munkáltatónak ki kell térnie többek között arra, hogy:

- milyen célból, milyen munkáltatói érdekek miatt kerülhet sor az e-mail fiók ellenőrzésére (illetve természetesen a konkrét ellenőrzés előtt tájékoztatni kell a munkavállalót arról, hogy milyen munkáltatói érdek miatt kerül sor az ellenőrzésre),
- a munkáltató részéről ki végezheti az ellenőrzést,
- milyen szabályok szerint kerülhet sor ellenőrzésre (fokozatosság elvének betartása) és mi az eljárás menete,
- milyen jogai és jogorvoslati lehetőségei vannak a munkavállalóknak az e-mail fiók ellenőrzésével együtt járó adatkezeléssel kapcsolatban.

A munkaállomás átadását követően a munkáltató gondoskodik az emailok törléséről.

### **A munkáltató által a munkavállaló rendelkezésére bocsátott laptop ellenőrzése**

A munkáltató bizonyos munkakörben dolgozó munkavállalók számára „céges laptopot, biztosít a munkájuk elvégzéséhez. A laptopot a munkavállalók saját, személyes céljaikra is használhatják. A laptopon elkülönítve kerül tárolásra a céges és a magán jellegű használat.

A laptopon tárolt adatokat a munkáltató ellenőrizheti.

A „céges laptop” tartalmának ellenőrzése illetve a laptop átadása esetében a munkáltatói **jogos érdek az adatkezelés jogalapja**. Ezen ellenőrzés esetében kiemelt figyelmet kell fordítani az célhoz kötött adatkezelés elvén és a szükségesség-arányosság követelményén túl az érintettek magánszférájára is, hiszen adott esetben különféle, a munkaviszonyhoz nem kapcsolódó személyes adat is a munkáltató tudomására juthat, illetve vele munkaviszonyban nem álló személyek adatait is megismerheti.

A munkáltatónak a laptop tartalmának ellenőrzése illetve átadása előtt közölnie kell a munkavállalóval, hogy pontosan milyen érdeke miatt kerül sor a munkáltatói intézkedésre. A munkáltatónak a fokozatosság elvére figyelemmel lépcsőzetes ellenőrzési rendszert kell kidolgoznia, amelyben megfelelően érvényesülhet a személyes adatok védelme, illetve hogy az ellenőrzés minél kisebb mértékben érintse a munkavállalók magánszféráját. A laptop tartalmának az ellenőrzése illetve átadása során ezért biztosítani kell a munkavállalók jelenlétét.

A laptop átadását követően a magán jellegű tartalmak törlésre kerülnek.

### **Az internethasználat ellenőrizhetősége**

A munkavállaló által meglátogatott weboldal vagy az internethasználatával kapcsolatban a számítógépen rögzített, lementett információk (például az elmentett felhasználónév, jelszó) a munkavállaló személyes adatainak tekinthetők. Ebből fakadóan a munkáltatónak a munkavállalók internethasználatával összefüggésben is tekintettel kell lennie az adatvédelmi követelményekre.

Az internethasználat ellenőrzése esetén szintén a munkáltatói jogos érdek lesz az adatkezelés jogalapja. A munkáltatónak előzetesen részletes tájékoztatást kell biztosítania a



munkavállalók számára az ellenőrzésről. A tájékoztatóban a munkáltatónak ki kell térnie többek között arra, hogy:

- hogy milyen célból, milyen munkáltatói érdekek miatt kerülhet sor az internethasználat ellenőrzésére (illetve természetesen a konkrét ellenőrzés előtt tájékoztatni kell a munkavállalót arról, hogy milyen munkáltatói érdek miatt kerül sor az ellenőrzésre),
- a munkáltató részéről ki végezheti az ellenőrzést,
- milyen szabályok szerint kerülhet sor ellenőrzésre (fokozatosság elvének betartása) és mi az eljárás menete,
- milyen jogai és jogorvoslati lehetőségeik vannak a munkavállalóknak az internet használatának ellenőrzésével együtt járó adatkezeléssel kapcsolatban.

### **A céges mobiltelefon , tablet használatának ellenőrizhetősége**

A társaság bizonyos munkakörökhöz személyes használatra céges mobil telefont illetve tabletet biztosít, melyhez a társaság által finanszírozott keretet határoz meg. A telefon, tablet magáncélra is használható.

A hivatalos hívások adatait a munkáltató megismerheti, a magáncélú hívások adatait nem.

A „céges mobiltelefon” használatának ellenőrzése esetén a munkáltatói jogos érdek az adatkezelés jogalapja. Az ellenőrzés nem terjedhet ki arra, hogy a munkavállalók magáncélból kit és mikor hívtak fel. Az ellenőrzésnél elengedhetetlen, hogy a munkáltató előzetesen részletes tájékoztatást biztosítson a munkavállalók számára. A tájékoztatóban a munkáltatónak ki kell térnie többek között arra, hogy:

- hogy milyen célból, milyen munkáltatói érdekek miatt kerülhet sor a „céges mobiltelefon” használatának ellenőrzésére,
- a munkáltató részéről ki végezheti az ellenőrzést,
- milyen szabályok szerint kerülhet sor ellenőrzésre és mi az eljárás menete,
- milyen jogai és jogorvoslati lehetőségei vannak a munkavállalóknak „céges mobiltelefon” ellenőrzésével együtt járó adatkezeléssel kapcsolatban.

A társaság bizonyos **munkahelyeken** céges mobiltelefont biztosít. Ezek a telefonok **magáncélra nem használhatóak. A társaság jogosult a magáncélú használatot ellenőrizni és annak térítési díját a munkavállalóval megfizettetni.**

### **WayQuest GPS alapú technológiai rendszerrel végzett nyomonkövetés**

A WayQuest rendszer ismertetését a melléklet tartalmazza.

A GPS navigációs rendszer által tárolt adat a gépjárművet vezető személyes adatának is minősül, minthogy annak alapján következtetéseket lehet levonni a munkavállalóra (például mikor, milyen útvonalon haladt a munkavállaló, mennyi idő alatt milyen távolságot tett meg).

A GPS alkalmazása logisztikai, munkaszervezési és vagyonvédelmi célból indokolt. A munkafolyamatok, és ezáltal közvetve a munkavállaló ellenőrzése kizárólag munkával, munkaszervezéssel, vagyonvédelemmel összefüggő célokat szolgálhat.

A GPS rendszer alkalmazása esetén a munkáltatói jogos érdek lesz az adatkezelés jogalapja.

Szükséges, hogy a munkáltató megfelelő tájékoztatást biztosítson a munkavállalók részére.

A GPS adatokat a növénytermesztési termelés irányítók naponta összevetik a munka elosztás során meghatározott feladatokkal, ellenőrzik a munkavégzés helyét és az üzemanyag felhasználást. Amennyiben a vizsgálat során eltérést, rendellenességet tapasztalnak kötelesek azt a vezérgazgatónak jelezni.

Amennyiben a GPS adatok alapján munkaügyi vétség gyanúja merül fel és ezért a munkáltató az Mt. 11. §-ával összhangban végez ellenőrzést, akkor a GPS adatok ismételt ellenőrzésére és összevetésére kerül sor. Ennek során a munkavállaló nyilatkozatot tehet és a GPS adatokat ellenőrizheti. Az ellenőrzés csak munkaidőben történhet és nem ellenőrizhető a munkavállalók földrajzi helyzete munkaidőn kívül. A munkavállalót az általános szabályok szerint megilleti a jogorvoslati lehetőség.

## **11. Nem munkaviszonyhoz kötődő személyes adatok védelme**

### **Adatkezelés célja:**

A társaság csak olyan személyes adatokat kezel (felvesz, rögzít, tárol) melyek tevékenységének ellátásához, feladatainak teljesítéséhez szükségesek. Az adatkezelés célja alapján az alábbi adatokat különbözteti meg a társaság:

- földterületek bérletéhez kapcsolódó adatok
- szerződéses, pénzügyi kapcsolatokhoz szükséges adatok
- vagyon és állatvédelemhez kapcsolódó adatok

### **Érintettek kategóriái:**

- földtulajdonosok, föld bérbeadók,
- szerződő partnerek, szállítók, vevők,
- a társaság területére látogatók,

### **Személyes adatok kategóriái:**

- név, születéskori név
- születési hely, idő
- anyja neve
- lakcím, tartózkodási hely
- állampolgárság
- adóazonosító jel
- személyi azonosító szám – kizárólag ingatlan nyilvántartáshoz kapcsolódó partnereknél
- vállalkozói igazolvány szám, nyilvántartási szám
- őstermelői igazolvány szám, adószám, értékesítési betétlap
- regisztrációs szám
- székhely, telephely
- adószám, közösségi adószám, csoport adószám
- pénzforgalmi adózás jelölése
- bankszámlaszám
- tulajdonát képező ingatlan adatai
- tulajdoni, hasznélvezeti arány
- kamera felvételek

### **Címzettek kategóriái:**

- NAV
- bíróság
- végrehajtók,
- önkormányzatok
- földhivatal

### **Törlési határidők**

- szerződéses partnerek adatai a szerződés lejárata követően az elévülési határidő végéig
- pénzügyi adatok - 10 év

### **Speciális adat kezelés:**

#### **Kamerás megfigyelés**

Jogszabály négy esetben teszi lehetővé az elektronikus megfigyelőrendszer alkalmazását:

- az emberi élet, testi épség, személyi szabadság védelme,
- a veszélyes anyagok őrzése,
- az üzleti, fizetési, bank- és értékpapírtitok védelme,
- vagyónvédelem.

A célhoz kötött adatkezelés elvéből fakadóan elektronikus megfigyelőrendszert alkalmazni elsődlegesen ezen célokból lehet, illetve a rögzített felvételek is ezen célokból használhatók fel. Az elektronikus megfigyelőrendszerek alkalmazhatóságának fontos feltétele, hogy semmiképp sem lehet kamerát elhelyezni olyan helyiségben, amelyben a megfigyelés az emberi méltóságot sértheti, így különösen az öltözőkben, zuhanyzóknak, az illemhelyiségekben vagy például orvosi szobákban, váróban.

A társaság elektronikus megfigyelőrendszert kizárólag a saját tulajdonában (vagy a használatában) álló épületrészek, helyiségek és területek, illetőleg az ott történt események megfigyelésére alkalmaz, közterület megfigyelésére azonban nem.

Az elektronikus megfigyelőrendszer által rögzített felvételek tárolásának időtartama maximum 6 hónap.

- az adatkezelés jogalapja: élet és testi épség védelme, vagyónvédelem, állatjóléti feltételeknek való megfelelés,
- a felvétel tárolásának helyét is időtartamát az adatok megismerésére jogosult személyek körét a melléklet tartalmazza,
- a felvételek visszánézésére a mellékletben meghatározott személyek jogosultak, amennyiben a jogalap sérelme feltételezhető és a felvételeket vagyón elleni cselekmények esetében a nyomozó hatóságoknak továbbíthatja.
- az érintett személyt megilleti a kamera felvételek visszánézésénél való részvétel joga, a kamera felvétel tárolási időt követő törlésének követelésére való jog, valamint a továbbításról való tájékoztatás joga. A jogok megsértése esetén az érintettek az általános adatvédelmi jogorvoslatra jogosultak.

### **III. Az adatkezelés elemei, fázisai**

#### **1. Az adat felvétele, rögzítése, feldolgozása**

**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;

A személyes adatokat a társaság az érintettek személyi okmányai alapján (személyi igazolvány, lakcím kártya, adókártya, TAJ kártya) veszi fel, rögzíti, dolgozza fel, illetve építi be a szerződésekbe. Az adatokat tartalmazó iratokról a Társaság másolatot készít, illetve a munkavállalók esetében azt szkennelt formában tárolja a munkaügyi program részeként.

Az adatok felvételére a vezérigazgató, a gazdasági igazgató, a szerződést kötő személy, a jogtanácsos, a munkaügyi csoport, valamint a pénzügyi és számviteli osztály jogosult.

A munkavállalók adatait adatlapon, szerződésben és a bérszámfejtéshez használt számítógépes programban ( NEXON) is rögzíti a munkaügyi csoport.

A szerződéses partnerek adatainak rögzítése a szerződésben és a társaság partner törzs adatbázisaiban történik. A társaság által készített, vagy hozzá érkező szerződések iktatásra és elektronikus tárolásra kerülnek az iktató programban, melyet a titkárnői feladatokat ellátó és a kiscsérpusztai adminisztrátori feladatokat ellátó személy végez.

A földtulajdonosok adatai a szerződésben, a partner törzs adatbázisokban és a földnyilvántartó programban is rögzítésre kerülnek. A társaság által készített, vagy hozzá érkező szerződések iktatásra és elektronikus tárolásra kerülnek az iktató programban melyet a titkárnői feladatokat ellátó és a kiscsérpusztai adminisztrátori feladatokat ellátó személy végez.

#### **2. A felvett adat megismerésére jogosultak köre:**

A társaság csak olyan személyes adatokat kezel, melyek tevékenységének ellátásához, feladatainak teljesítéséhez szükségesek.

Az adatkezelés célja:

- munkaviszony létesítése, teljesítése fenntartása ( foglalkoztatás), megszüntetése
- társadalombiztosítási kifizetések teljesítése ( TB kifizető hely)
- törvényi előírások teljesítése (adó törvények, munkavédelmi törvény, stb)
- földterületek bérlete
- szerződések létesítése, teljesítése,
- pénzügyi kapcsolatok teljesítése
- vagyonvédelem
- önkéntes pénztári belépés

- kollektív szerződés alapján járó juttatások biztosítása
- tovább képzések
- társaság jogos érdekének biztosítása

Munkaviszonnal kapcsolatos személyes adatokat a vezérigazgató, a gazdasági igazgató, a munkaügyi csoport, a jogtanácsos, a munkáltatói jog gyakorlója, a számviteli és pénzügyi osztály ismerheti meg.

A szerződéses adatokat a vezérigazgató, a gazdasági igazgató, jogtanácsos, a pénzügyi és számviteli osztály, illetve a szerződéssel érintett terület vezetői ismerhetik meg.

A földtulajdonosok adatait a vezérigazgató, a gazdasági igazgató, a jogtanácsos, a pénzügyi és számviteli osztály, valamint a földügyi ügyintéző ismerheti meg.

### **3. A felvett adat továbbítása**

Adat továbbítására csak a szabályzatban meghatározott címzettek részére kerülhet sor. Az adat továbbításáról a munkaügyi csoport a pénzügyi és számviteli osztály illetve a jogtanácsos rendelkezhet.

#### **Címzettek kategóriái:**

- NAV
- foglalkozás egészségügyi szolgálat
- önkéntes nyugdíjpénztár
- nyugdíj és egészségbiztosítási pénztár, igazgatóság
- bíróság
- végrehajtók,
- önkormányzatok
- földhivatal
- kamarák
- bankok
- iskolák képző helyek
- kollektív szerződés alapján nyújtott juttatás szolgáltatója
- NEXON bérprogram üzemeltetője

### **4. A felvett adat javítása, helyesbítése**

Az adatkezelés során biztosítani kell az **adatok pontosságát, teljességét** és - ha az adatkezelés céljára tekintettel szükséges - **naprakészségét**, minden ésszerű intézkedést meg kell tenni annak érdekében, hogy az adatkezelés céljából pontatlan személyes adatok haladéktalanul törlésre vagy javításra kerüljenek. A társaság amennyiben észleli az adat pontatlanságát, hibáját saját elhatározásból is módosíthatja azt, illetve az érintett a helyesbítést módosítást kérheti.

## **5. Törlés**

**Az adat törlése** az adat felismerhetetlenné tétele oly módon, hogy a helyreállítása többé nem lehetséges. Törlésre vagy a tárolási határidő végén automatikusan, vagy az érintett kérelmére kerülhet sor.

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.

Ha a személyes adat a valóságnak nem felel meg, és a valóságnak megfelelő személyes adat az adatkezelő rendelkezésére áll, a személyes adatot az adatkezelő helyesbíti.

A személyes adatot törölni kell, ha

- a) kezelése jogellenes;
- b) az érintett - a 14. § c) pontjában foglaltak szerint - kéri;
- c) az hiányos vagy téves - és ez az állapot jogszerűen nem orvosolható -, feltéve, hogy a törlést törvény nem zárja ki;
- d) az adatkezelés célja megszűnt, vagy az adatok tárolásának törvényben meghatározott határideje lejárt;
- e) azt a bíróság vagy a Hatóság elrendelte.

Törlés helyett az adatkezelő zárolja a személyes adatot, ha az érintett ezt kéri, vagy ha a rendelkezésére álló információk alapján feltételezhető, hogy a törlés sértené az érintett jogos érdekeit. Az így zárolt személyes adat kizárólag addig kezelhető, ameddig fennáll az az adatkezelési cél, amely a személyes adat törlését kizárta.

## **IV. A papír alapon rögzített adatok védelme**

Személyes adatokat tartalmazó iratokat a jogtanácsos, a munkaügyi csoport és a pénzügyi és számviteli osztály valamint az irattár tárolhat. A tárolás tűz, villám védelemmel és riasztó ellátott épületben, biztonsági zárral ellátott helységben, zárható szekrényben történik. Az iratok megtekintésére kizárólag azok a munkavállalók jogosultak, akiknek munkájához az adatok megismerése kezelése szükséges.

## **V. A számítás technikai rendszerben rögzített adatok védelme, az adatvédelem technikai eszközei és szabályai**

## 1. A számítástechnika működtetésének szervezeti felépítése

### Vezérigazgató helyettes

A **vezérigazgató helyettes** meghatározza a számítástechnikai rendszer fő feladatait, részt vesz a számítástechnikai fejlesztések meghatározásában, biztosítja a fejlesztések pénzügyi fedezetének rendelkezésre állását. Irányítja a számítástechnikai rendszerszervező és a számítástechnikus munkáját.

- Rendszeresen ellenőrzi a jelen szabályzatban foglaltak végrehajtását, betartását.
- Rendszeresen ellenőrzi a védelmi eszközökkel való ellátottságot.
- Ellenőrzi az informatikai munkafolyamat bármely részét.
- Ellátja az adatkezelés és feldolgozás felügyeletét.

### Számítástechnikai rendszerszervező

A társaság számítástechnikai rendszerének kialakítása, működtetése a számítástechnikai rendszerszervező feladata. A számítástechnikai rendszerszervező a gazdasági igazgató irányítása alatt működik. A számítástechnikai rendszerszervezőnek közvetlen beosztottja nincsen, azonban számítástechnikai szempontból az adatrögzítők, illetve a számítógépeket kezelő egyéb személyek felé utasítási joga van.

A számítástechnikai rendszerszervező feladatai:

- A társaságban megvalósítandó számítástechnikai fejlesztésekre vonatkozó javaslatok elkészítése.
- A jóváhagyott fejlesztések bevezetésének folyamatos biztosítása.
- Részt vesz a számítógépes feldolgozáson alapuló komplex integrált információs rendszer kialakításában.
- Biztosítja a bevezetett számítástechnikai rendszerek folyamatos üzemeltetésének lehetőségét.
- Gondoskodik a számítástechnikai eszközök és saját fejlesztésű programok használhatóságáról, karbantartásáról. Biztosítja a jelentkező hibák kijavítását, illetve kijavíttatását.
- Segíti a számítástechnikai feldolgozások előkészítését.
- Biztosítja a rendszer működéséhez szükséges adathordozókat és egyéb szükséges anyagokat.
- Biztosítja a számítógépes adatok mentését.
- Kapcsolatot tart minden hardver és szoftverszállítóval.
- Felelős az informatikai rendszer üzembiztonságáért, a szerverek adatairól biztonsági másolatok készítéséért és karbantartásáért.
- Gondoskodik a rendszer kritikus részeinek újra indíthatóságáról, illetve az újra indításhoz szükséges paraméterek reprodukálhatóságáról.
- Feladata a védelmi eszközök működésének folyamatos ellenőrzése.
- Nyilvántartja a beszerelt, illetve üzemeltetett hardver és szoftver eszközöket.
- Gondoskodik a folyamatos vírus védelemről.
- Vírus fertőzés gyanúja esetén gondoskodik a vírusmentesítésről.
- A gazdasági igazgatóval és a pénzügyi és számviteli osztályvezetővel való folyamatos egyeztetés mellett részt vesz a havi zárlati feladatok elvégzésében

Határidőhöz kötött havi rendszerességgel ismétlődő feladatok:

- Minden hónap 8. napjáig köteles a főágazatok műhely és segédüzemi felosztóinak elkészítésében, a havi segédüzemi feladatok lekérdezésében közreműködni.
- Minden hónap 8. napjáig köteles a munkaügyi csoport részére a bérfelosztáshoz szükséges munkaidőadatokat rendelkezésre bocsátani.
- Minden hónap 14. napjáig köteles a továbbszámításra kerülő előző havi mobiltelefon számla adatait a szolgáltató által biztosított jelentés alapján a számlázáshoz szükséges formátumban a pénzügyi csoportnak átadni.

### Számítástechnikus

- Közreműködik a társaságban folyó számítástechnikai, informatikai fejlesztések bevezetésében.
- LynxPFők (pénzügyi-főkönyvi) LynxBesz (tárgyi eszköz és immateriális javak) LynxPtár (házi pénztár) LynxTerv (terv-tény elemző) és a LynxPter (pénzügyi terv-tény elemző) szoftverek, illetve a földnyilvántartó program folyamatos karbantartása, aktualizálása, működőképességének biztosítása, a felmerülő új igényeknek megfelelő módosítások végrehajtása.
- A gazdasági igazgatóval és a pénzügyi és számviteli osztályvezetővel való folyamatos egyeztetés mellett részt vesz a havi zárlati feladatok elvégzésében

Határidőhöz kötött havi rendszerességgel ismétlődő feladatok:

- Minden hónap 9. napjáig köteles a készletprogram főkönyvi feladását elvégezni, az esetleges hibajavításokat a készletkezelők, illetve a számviteli csoportvezető bevonásával elvégezni.
- Minden hónap 13. napjáig köteles a takarmánykeverő havi készletérték különbözetének felosztását a pénzügyi és számviteli osztályvezetőnek elkészíteni.
- Minden hónap Általános Forgalmi Adó bevallásának elkészítésében a pénzügyi és számviteli osztályvezető irányításával köteles részt venni az adott havi bevallási határidő betartásával.

## **2. A számítástechnikai rendszer védelme**

A társaság számítógépes rendszerének védelme magában foglalja a vagyonvédelmi, a tűzvédelmi és az adat- titokvédelmi szabályokat egyaránt. A számítástechnikai védelmi szabályokat a társaság valamennyi munkavállalója köteles betartani. A számítástechnikai védelmi szabályokat alkalmazni kell a társaság tulajdonában lévő valamennyi számítástechnikai berendezésre és az ehhez kapcsolódó eszközökre, valamint a számítástechnikai rendszerben szereplő valamennyi adatra.

### *1. Védelmet igénylő adatok, eszközök köre:*

- A számítástechnikai eszközökben, programokban tárolt személyes adatok
- A számítástechnikai eszközökben, programokban tárolt társasági adatok
- A számítógépes adatfeldolgozásban alkalmazott hardver eszközök és azok működési biztonsága.
- A számítástechnikai eszközök üzemeltetéséhez szükséges okmányok és dokumentációk.
- Az adatok, adathordozók a megsemmisítésükig, illetve a közlésre szánt adatok felhasználásáig.



- Az adatfeldolgozó programrendszerek, valamint a feldolgozást támogató rendszer szoftverek tartalmi és logikai egysége előírászerű felhasználása, reprodukálhatósága.
- Az alkalmazott biztonsági intézkedések, azok tervei, tartalmi előírásai és eljárási szabályai.

## 2. *A számítástechnikai eszközöket és adatokat veszélyeztető helyzetek, események:*

### 2.1. A számítástechnikai eszközöket veszélyeztető helyzetek

Az információk előállítására, feldolgozására, tárolására, továbbítására, megjelenítésére alkalmas számítógépek és egyéb számítástechnikai berendezések fizikai károsodását okozó események.

#### a.) Elemi csapások és környezeti ártalmak:

- Elemi csapások: mint földrengés, árvíz, villámcsapás, stb.
- A környezetből származó károsító hatások: légszennyezettség, nagy elektromágneses térerő jelenléte, elektrosztatikus feltöltődés, fokozott tűz- és robbanásveszély, levegő nedvességtartamának változása, por.
- Közüzemi szolgáltatásokban keletkezett zavarok: feszültség kimaradás, feszültség ingadozás, fűtés leállás, légkondicionáló leállás, elektromos zárlat, csőtörés

#### b.) Emberi tényezőkre visszavezethető veszélyek:

##### Szándékos károkozás

- Behatolás a számítástechnikai rendszerek közvetlen közelébe.
- Illetéktelen hozzáférés az adatokhoz, eszközökhöz.
- Az adatok, eszközök eltulajdonítás, visszaélészerű használata.
- A gépek, berendezések, adathordozók rongálása, működésük használhatóságának korlátozása.
- Megtévésztő adatok rendszerbe vitele, képzése.
- A feldolgozások és munkafolyamatok zavarása, késleltetése.

##### Nem szándékos, illetve gondatlan károkozás

- Fegyelmezetlenség, ellenőrzés hiánya.
- Szakmai hozzá nem értés, szakmai összefüggések fel nem ismerése.
- A gépi és eljárásbeli biztosítékok számítástechnikai rendszerekbe történő beépítésének elhanyagolása.
- Illegális másolattal vírusfertőzött szoftver behozatala.
- Biztonsági követelmények megrongálódása.
- A karbantartási műveletek elmulasztása.
- A szükséges biztonsági jelző, és riasztó berendezések elhanyagolása.

### 2.2. Az adattartalmat és a feldolgozás folyamatát érintő veszélyek:

- a) A számítástechnikai rendszerek tervezése és előkészítése során előforduló veszélyforrások:
- A rendszerterv nem minden részletre kiterjedően veszi figyelembe az alkalmazott számítástechnikai berendezések hardver lehetőségeit.
  - A rendszerterv az adatvédelmi szempontok hiányos figyelembe vételével készült.

- b) A számítástechnikai rendszerek megvalósítása során előforduló veszélyforrások: hibás adatállomány működtetés, helytelen adatkezelés, program működésének hiányos ellenőrzése.
- c) A számítástechnikai rendszer működése és fejlesztése során előforduló veszélyforrások: emberi gondatlanság, szervezetlenség, képzetlenség, üzemeltetési dokumentáció hiánya, illetéktelen beavatkozás.

### 3. A számítástechnikai eszközök és adatok védelmének szabályai

#### 3.1. Számítástechnikai eszközök védelme

##### a.) Vagyonvédelmi előírások:

A számítástechnikai eszközöket fokozott védelemben kell részesíteni, kiemelten kell kezelni a szerver számítógépet. Valamennyi számítógépet befogadó helyiséget zárral kell ellátni. Az illetéktelen behatolás tényét azonnal jelenteni kell a vezérigazgatónak és a számítástechnikai rendszerszervezőnek. A különböző irodahelyiségekben elhelyezett számítástechnikai eszközöket csak a kinevezett, illetve kijelölt, azok kezelésére és védelmére kioktatott személyek használhatják. A felhasználó a géphasználat ideje alatt a számítástechnikai eszközök rendeltetésszerű működtetéséért egy személyben felelős.

Az adathordozókat könnyen tisztántartható, jól zárható szekrényekben kell elhelyezni úgy, hogy tárolás közben ne sérüljenek, károsodjanak. Az irodai helyiségekből bármilyen adathordozót, adatállományt más intézménynek átadni csak az illetékes vezető engedélyével lehet.

##### b.) Tűzvédelmi előírások:

Számítástechnikai eszközöknél oltóanyagként halon-gázt, vagy habot szabad alkalmazni. A tűzoltó készülékek üzemképességének vizsgálatát rendszeresen el kell végezni.

A számítástechnikai eszközök környezetében csak annyi papír tárolható, amennyi az aktuális feldolgozáshoz szükséges. A számítástechnikai eszközök környezetében tűzveszélyes folyadékot tárolni tilos!

Azokat a törzsadat állományokat, melyeknek megsemmisülése jelentős kárt okozna, két példányban kell őrizni külön-külön helyen.

##### c/ Káresemény esetén felhasználható védelmi eszközök és módszerek:

###### Irodahelyiségek védelme

Elemi csapás, vagy az irodahelyiségek részleges, vagy teljes károsodásakor a szükséges teendők a következők:

- Menteni a még használható anyagokat.
- A megsérült adatok visszaállítása a háttértárolókról biztonsági mentésekről.
- Az új adatfeldolgozási helyiségek kialakítása.
- Az archivált anyagok felhasználásával mielőbb folytatni kell a feldolgozást.

### Hardver védelem

Vihar esetén a villámcsapás okozta károsodás elkerülése érdekében, a szünetmentes tápegységeket áramtalanítani kell. A munkaidő befejezésekor a károsodás megelőzése érdekében a gépeket ki kell kapcsolni, és áramtalanítani kell.

A számítástechnikai berendezések hibátlan és üzemszerű működését biztosítani kell. A működési biztonság megóvását segíti a szükséges alkatrészek beszerzése. A rendszeres karbantartási munkákat előre tervezetten, körültekintően és gondosan kell elvégezni. A karbantartási munkák szervezésénél figyelembe kell venni: a gyártó előírásait, ajánlásait, az üzemeltetés tapasztalatait, a hardver-tesztek által feltárt hibákat. A karbantartás idejét úgy kell megállapítani, hogy az emiatt kieső idő a legkevésbé legyen zavaró a felhasználók részére.

### 3.2. Az alkalmazás folyamatának védelme

A számítástechnika alkalmazás folyamatában az adatvédelem kiemelt fontosságú, mivel a folyamat során a meglévő, illetve a kialakításra kerülő adatállományok sérülésének lehetősége nagy.

#### Az adatbevitel védelme

Csak hibátlan műszaki állapotú berendezéseken történhet adatbevitel. Csak letesztelt adathordozókra lehet adatállományt rögzíteni. A mágneses adathordozókat csak az e célra kialakított, megfelelő tárolóban szabad tárolni. Az adatbevivő berendezés minden ellenőrző lehetőségét ki kell használni. Az adatbevivő programokat ellenőrző funkciókkal kell ellátni. Biztosítani kell a rögzített tételek visszakeresésének és javításának lehetőségét. Az adatokhoz, információkhoz való hozzáférést a számítógépes feldolgozási rendszerben a bejelentkezési azonosítók használata teszi lehetővé. Az azonosítókkal elhatárolható, hogy milyen adatokhoz, milyen szinten lehet hozzáférni. A bejelentkezési azonosítókat a társaság számítógépes rendszerszervezője köteles nyilvántartani. A hálózatos rendszerbe történő belépés előtt a bejelentkezési azonosítót és a jelszót is be kell gépeltetni. A belépési jelszavak nyilvántartása szintén a számítógépes rendszerszervező feladata. A jelszavak frissítése alapvető rendszervédelmi feladat. A számítógépes hálózatba nem kapcsolt egyedi munkahelyen a feldolgozásnak megfelelően kell kialakítani a bemenő adatok védelmét.

#### Adathordozók védelme

Az adathordozók logikai védelmét az operációs rendszer és az ehhez tartozó ellenőrző file kezelő rutinok alkalmazásával kell biztosítani.

Az adathordozók szállítása csak megfelelően körültekintő módon a szállítás során előforduló környezeti veszélyforrások figyelembe vételével lehetséges.

Az adathordozókon tárolt adatok megőrzési idejét az üzemeltető és a felhasználó közösen határozzák meg. A megőrzési idők nyilvántartásáért és ezek betartásáért a számítástechnikai rendszerszervező a felelős.

Selejtezni kell az adathordozót: javíthatatlan fizikai károsodás, gyári, gyártási, raktározási hibából eredő alkalmatlanság, végleges elhasználódás esetén. A további felhasználásra alkalmatlan adathordozókat fizikai roncsolással kell használhatatlanná tenni.

### Felhasználói programok védelme

A számítógépes programokat megfelelő tárolás és nyilvántartás mellett kell kezelni. A kezelés folyamán az illetékes hozzáférést biztosítani kell, az illetéktelen hozzáférést pedig ki kell zárni. A programok védelmének megvalósítása során gondoskodni kell arról, hogy a tárolt programok ne károsodjanak. A feldolgozás biztonságának megvalósítása érdekében naprakész állapotban kell tartani a program dokumentációt, mert a felismert hibák javítását csak ennek birtokában lehet elvégezni. A felhasznált programokról nyilvántartást kell vezetni. A nyilvántartást úgy kell kialakítani, hogy abból egyértelműen megállapíthatók legyenek a program azonosítására és kezelésére vonatkozó adatok.

### Központi számítógépek védelme

A központi számítógép elektromos hálózati betáplálásánál szünetmentes tápegységet kell alkalmazni, ami megvédi a berendezéseket a hálózati feszültség ingadozásoktól és áramkimaradás esetén is lehetővé teszi a hálózat biztonságos adatvesztés nélküli leállítását. A központi számítógép változásairól naponta mentést kell végezni. Havonta egyszer teljes mentést kell készíteni. A biztonsági mentés elkészítését folyamatosan aktualizált szoftverekkel végzett vírusesztnak és mentésítésnek kell megelőznie. A biztonsági mentéseket tartalmazó adathordozókat, valamint a rendszerprogramok másolatát illetéktelen behatolás, tűz, vagy elemi csapás ellen egyaránt védelmet nyújtó helyen kell tárolni. A vásárolt szoftver eszközökről, amennyiben ez lehetséges, biztonsági másolatot kell készíteni. Az eredeti példányokat a másolatoktól fizikailag elkülönítetten kell tárolni.

### Munkaállások védelme

A vírusfertőzés lehetőségének minimálisra csökkentése érdekében a hálózatra kapcsolódó számítógépekre idegen programot, adatot másolni, vagy bármi egyéb módon bejuttatni csak egyeztetés és ellenőrzés után lehet. Ilyen programot kizárólag a legújabb vírusesztelési eljárás után szabad felhasználni. A vírusvizsgáló programnak minden számítógépen ott kell lennie és azt minden hajlékony, optikai lemez, és pendrive használata előtt le kell futtatni. Vírusfertőzés gyanúja esetén haladéktalanul a rendszert izolálni kell, le kell választani a számítógép hálózatról. Közvetlen Internet kapcsolattal rendelkező számítógépek esetén biztosítani kell a folyamatos vírusvédelmet. (Online vírusölő programok). A hálózat biztonságos működésének érdekében a hálózat felhasználói számára rendelkezésre bocsátott háttértár területeken olyan szoftvert futtatni, ami a hálózat operációs rendszere által létrehozott háttértár struktúráját átrendezi, tilos. Új rendszereket használatbavételük előtt szükség szerint adaptálni szükséges, és teszt adatokkal ellenőrizni kell helyes működésüket. Mágneses adathordozókat használaton kívül eredeti csomagolásukban, vagy az ezekhez készült tároló dobozokban, illetve szekrényekben, hőtől, elektromágneses terektől távol, száraz és pormentes helyen kell tárolni.

A hálózat vezetékeinek számítógépéinek felhasználók által történő mindennemű megbontása tilos. A számítógépek, illetve az operációs rendszerek beállításain, paraméterein változtatni csak a számítástechnikai rendszerszervezővel történt egyeztetést követően lehet. Számítástechnikai eszközt és tartozékát helyéről a munkahelyi vezető engedélye nélkül, elvinni tilos. A társaság által a munkavállalója

részére rendelkezésre bocsátott számítástechnikai eszköz kizárólag munkavégzésre használható. A használatot a társaság ellenőrzi.

#### **4. Az adatmentés szabályai**

Adatmentésen a számítógépen tárolt programok és adatok olyan háttértárra történő másolását értjük, amit a másolás után tárolni kell.

##### *1. Vásárolt programok kezelése*

A vásárolt programok háromféle adathordozón kerülhetnek a társaságba: CD, mágneslemez, Internet. A programok kezelése az adathordozóktól függetlenül a következő:

##### CD, DVD, BD, PD, külső SSD, HDD lemez esetén

A lemezen található installáló anyag az adathordozóból adódóan felülírás ellen védett. Az installálást a vásárolt eredeti lemezről elvégezzük, majd az erre kijelölt helyen tároljuk.

##### Mágneslemez esetén

Az így kapott telepítő lemezekről azonnal egy munkakópiát kell készíteni. Az eredeti lemezeket lezárt, külön helyen kell elhelyezni, a programok telepítése csak az írásvédelemmel ellátott munkakópiáról történhet.

##### Internet esetén

Interneten érkező programot közvetlenül kell telepíteni. A letöltésről azonnal egy munkakópiát kell készíteni. A munkakópiát külön helyen kell tárolni.

Minden adathordozón esetén érvényes előírások:

- telepítő anyagot (munkakópiát is) kiadni tilos
- pontos nyilvántartást kell vezetni a felhasználói licencekről
- csak jogtiszt programok üzemeltethetők

##### *2. File szerverek adatmentése*

A központi gépet több winchesterrel kell ellátni, amelyeket raid rendszerben kell üzemeltetni.

A számítógép operációs rendszere biztosítja a lehetőséget, hogy a menteni kívánt adatokról automatikusan másolat készíthető legyen. A mentést a rendszerrel automatizálhatjuk.

A felhasználói programok adatbázisainak mentését az Ágostonpusztai, illetve a Kiscséripusztai file szerveren naponta, egy erre kijelölt gép automatikusan elvégzi olyan módon, hogy az adatbázisokat NAS-ra menti napi bontásban. A napi mentésre kijelölt adatállományok listáját a szabályzat 1. számú melléklete tartalmazza. A mellékletben szereplő állományok listáján bármilyen módosítás a gazdasági igazgató engedélyével történhet. A napi mentések havonta íródnak felül.

Az SQL szerverről napi mentés készül automatikusan Nas-ra , ami hetente íródik felül.

A Mail szerverről naponta automatikus mentés történik NAS-ra. A mentés az előző naphoz képest történt változásokkal szinkronizálja az előző nap mentését.

A szerver gépekről évente 1-2 alkalommal külön archiválás folyik SSD meghajtóra, aminek a végrehajtásáért a számítástechnikai rendszerszervező a felelős.

Az éves beszámoló elfogadása után a társaság teljes előző évi könyvelési adatait SSD-re rögzíti, amelyeket a gazdasági igazgató köteles pénzügyi értékmegőrzőben elhelyezni.

A bérelszámoláshoz szükséges adatokat a napi és heti mentések mellett a bérelszámolás elkészítése után külön is kell archiválni, ennek az elvégzéséért a munkaügyi csoport a felelős.

Az egyéb rendszerek által előírt különböző mentési eljárásokat a rendszerek leírása tartalmazza, itt nem szükséges szabályozni.

### *3. Adatmentés az üzemelő PC-kről*

A napi munka elmentése a számítógépre, vagy a központi szerverre a vele dolgozó munkatárs feladata. Az egyes számítógépeken tárolt adatok CD, DVD lemezre, SSD-re mentése a számítástechnikai rendszerszervező feladata.

Jelen szabályzat kiadásának napjától visszavonásig érvényes.

Ágostonpuszta, 2022. február 15.

Szávay Gábor  
vezérigazgató

## Nyilatkozat

Alulírott \_\_\_\_\_ (sz: \_\_\_\_\_, an:  
\_\_\_\_\_, beosztás: \_\_\_\_\_) munkavállaló

kijelentem,

hogy az Enyingi Agrár Zártkörűen működő Részvénytársaság tulajdonát képező számítógépeken kizárólag a társaság által hivatalos forgalmazóktól vásárolt és a társaság központi irányítása által rendelkezésre bocsátott szoftvereket alkalmazok.

Ágostonpuszta, 20\_\_\_\_\_

\_\_\_\_\_  
alíírás

## N y i l a t k o z a t

Alulírott \_\_\_\_\_ (sz: \_\_\_\_\_, an:  
\_\_\_\_\_, beosztás: \_\_\_\_\_) munkavállaló

k i j e l e n t e m,

hogy az Enyingi Agrár Zártkörűen működő Részvénytársaság Adatvédelmi és Kezelési Szabályzatában foglaltakat megismertem, munkámat az abban foglaltaknak megfelelően végzem.

Ágostonpuszta, 20 \_\_\_\_\_

\_\_\_\_\_  
aláírás





1. számú melléklet.

A Számítástechnikai szervezeti és védelmi szabályzat alapján naponta mentésre kerülő adatállományok:

**1. Az ágostonpusztai szerverek mentésre kijelölt állományai:**

\\Fserv\_agoston\sys\apéh  
\\Fserv\_agoston\sys\Develop\éles  
\\Fserv\_agoston\sys\dokumentumok  
\\Fserv\_agoston\sys\kut  
\\Fserv\_agoston\sys\torz\TO21  
\\Fserv\_agoston\sys\torz\TO22  
\\Fserv\_agoston\sys\Munkaköri\_leírás\Munkaköri 2022  
\\Fserv\_agoston\sys\netinfo  
\\Fserv\_agoston\sys\Nexonbér  
\\Fserv\_agoston\sys\segeduzem\su  
\\Fserv\_agoston\sys\segeduzem\traktor\TRAK2022  
\\Fserv\_agoston\sys\terv  
\\Fserv\_agoston\sys\titkarsag  
\\Fserv\_agoston\sys\util

**Mentés helye :**

Ágostonpuszta NAS

**2. A kiscsérpusztai szerverek mentésre kijelölt állományai:**

\\FSERV\_CSERI\konyvel\penztar  
\\FSERV\_CSERI\konyvel\traktor\Trak 2022  
\\FSERV\_CSERI\konyvel\penztar  
\\FSERV\_CSERI\koz\1 ÁLLATJÓLÉTI pályázat  
\\FSERV\_CSERI\koz\1 SPERMA IGÉNY  
\\FSERV\_CSERI\koz\2021-év  
\\FSERV\_CSERI\koz\2022-év  
\\FSERV\_CSERI\koz\Állategészségügy  
\\FSERV\_CSERI\koz\Attila\2022 év  
\\FSERV\_CSERI\koz\Bartyik  
\\FSERV\_CSERI\koz\Gábor  
\\FSERV\_CSERI\koz\Guba  
\\FSERV\_CSERI\koz\Hadi János  
\\FSERV\_CSERI\koz\Inszeminátorok  
\\FSERV\_CSERI\koz\KATI  
\\FSERV\_CSERI\koz\Kornél  
\\FSERV\_CSERI\koz\Lepsény  
\\FSERV\_CSERI\koz\riska  
\\FSERV\_CSERI\koz\riskom

\\FSERV\_CSERI\kozos\risku  
\\FSERV\_CSERI\kozos\Winsproc  
\\FSERV\_CSERI\kozos\Zsuzsa  
\\FSERV\_CSERI\kozos\Állatorvosok  
\\FSERV\_CSERI\kozos\Fanni  
\\FSERV\_CSERI\kozos\Zolnai Feri

**Mentés helye :**  
Kiscséri NAS